EDD Employment
Development
Department
State of California

**Employment
Development
Department**

State of California

Disability Insurance Branch Automation Project, Phase 3

Feasibility Study Report

Date: June 28, 2005

Revised: November 30, 2005

Project Sponsor:

FSR Registration No: 2004-01

Prepared by:

eskelporter
consulting, inc.

and

HSC
HUBBERT SYSTEMS CONSULTING

Table of Contents

Appendices

1.0 EXECUTIVE PROJECT APPROVAL TRANSMITTAL

Information Technology Project Request

Feasibility Study Report

Executive Approval Transmittal

Department Name		
California Employment Development Department		

Project Title (maximum of 75 characters)		
Disability Insurance Branch Automation Project		

Project Acronym	Department Priority	Agency Priority
DIAP3	1	

APPROVAL SIGNATURES		

I am submitting the attached Feasibility Study Report (FSR) in support of our request for the Department of Finance's approval to undertake this project.

I certify that the FSR was prepared in accordance with State Administrative Manual Sections 4920-4930.1 and that the proposed project is consistent with our information technology strategy as expressed in our current Agency Information Management Strategy (AIMS).

I have reviewed and agree with the information in the attached Feasibility Study Report.

Deputy Director, Information Technology Branch	Date Signed
Printed name:	
Budget Officer	Date Signed
Printed name:	
Department Director	Date Signed
Printed name:	
Secretary, Labor and Workforce Development Agency	Date Signed
Printed name:	

2.0 INFORMATION TECHNOLOGY PROJECT SUMMARY PACKAGE

2.1 Section A: Executive Summary

1	Submittal Date	06/15/2005			

		FSR	SPR	PSP Only	Other:
2	Type of Document	✓			
	Project Number	2004-01			

				Estimated Project Dates	
				Start	**End**
3	Project Title	Disability Insurance Branch Automation Project-Phase 3			
	Project Acronym	DIAP3		07/01/06	06/30/09

4	Submitting Department	Employment Development Department
5	Reporting Agency	Labor and Workforce Development

Project #	2004-01
Doc. Type	FSR

6	**Project Objectives**

The DIB Strategic Business Plan describes its goal of offering multiple communication methods to increase customer satisfaction. The DIAP3 will implement HIPAA-compliant electronic communications through the direct e-interface and Web-based intelligent forms, creating two new intake channels to assist DIB in meeting its access objectives. New intake methods will increase self-service options that allow claimants to be more responsible for providing DIB accurate and complete claim information through edits and business rules that promote accuracy and completeness of information received. The DIAP3 solution will also assist DIB in managing fraud and abuse through automated programs and business logic. The solution will detect unauthorized access to the PHI under EDD's ownership immediately upon implementation of the proposed solution, and automatically notify EDD of all unauthorized access or attempted access to PHI.

The Disability Insurance Automation Project, Phase 3 (DIAP3) includes adopting HIPAA guidelines and practices to accomplish further simplification and automation of DIB's numerous manual work processes. DIAP3 introduces proven technologies and builds on existing information technology systems to establish a secure electronic communications and information processing environment that will:

- Improve access to services

- Improve service delivery

- Detect and prevent fraud and abuse

Project #	2004-01
Doc. Type	FSR

7	**Proposed Solution**

The foundation of the DIAP3 solution is the implementation of a secure electronic communications and information processing environment that promotes efficiency and reduces costs by following HIPAA regulations and guidelines. HIPAA affords DIB an opportunity to realize the advantages of electronic communications with claimants, medical providers, and employers. Currently, key data entry (KDE) of paper documents is the only intake method for DI claims. DIAP3 will allow claimants, medical providers, and employers to use the Internet to submit claims data using a direct electronic interface or through web-based intelligent forms. Scanning/optical character recognition (OCR) will be implemented to convert remaining paper claims to electronic format. KDE will only be used for exception processing for a small percentage of paper forms that are not accepted in the scanning process. The DIB believes new intake methods will reduce KDE of paper forms from 100% to a single-digit percentage by the fifth year of DIAP3 solution operation. The following diagram illustrates DIB's evolution to an electronic data environment.

The DIB intends to undertake a business-based procurement to solicit technical solutions from vendors. Once a vendor proposal is accepted and costs are finalized, DIB will complete and submit a Special Project Report (SPR) to DOF describing the selected solution, scope of work, and costs.

Project #	2004-01
Doc. Type	FSR

8	Major Milestones	Est Complete Date
	Begin contracts for procurement assistance (PA), independent project oversight (IPO), and independent validation and verification (IV&V)	7/03/06
	Final RFP for systems integrator (SI)	10/27/06
	Special Project Report (SPR)	4/6/07
	Obtain DOF/OTROS SPR approval	6/20/07
	DGS issue Intent to Award SI contract	6/22/07
	Begin PM consultant contract	6/29/07
	Begin SI contract	7/2/07
	DIAP3 Design Solution Phase	11/30/07
	DIAP3 Develop and Test Solution Phase	12/12/08
	DIAP3 Deploy Solution Phase	6/30/09

Project #	**2004-01**
Doc. Type	**FSR**

Key Deliverables	Planned Delivery Date
PA vendor status reports	7/14/06—8/27/07
IPO status reports	7/14/06—6/29/09
IV&V status reports	7/14/06—6/29/09
SI status reports	7/6/07—6/29/09
SI Work Plan and Schedule	7/11/07
SI Project Management Plan with Project Charter	07/17/07
Monthly DIAP3 Steering Committee review	8/15/07—6/15/09
Design sign-off	11/30/07
.Net applications sign-off	9/5/08
Security sign-off	9/12/08
Electronic interface sign-off	9/16/08
Intelligent forms sign-off	9/18/08
Integration sign-off	9/18/08
Complete system test sign-off	10/2/08

Key Deliverables	Planned Delivery Date
Scanning/OCR sign-off	11/13/08
BPR sign-off	12/12/08
Training complete	4/3/09
Implementation sign-off	5/29/09
Support sign-off	6/30/09
9 **PIER**	**06/30/2011**

2.2 Section B: Project Contacts

Project #	2004-01
Doc. Type	FSR

<table>
<tr><th colspan="9">Executive Contacts</th></tr>
<tr><th></th><th>First Name</th><th>Last Name</th><th>Area Code</th><th>Phone #</th><th>Ext.</th><th>Area Code</th><th>Fax #</th><th>E-mail</th></tr>
<tr><td>Agency Secretary</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Dept. Director</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Budget Officer</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>CIO</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Proj. Sponsor</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="9">Direct Contacts</th></tr>
<tr><th></th><th>First Name</th><th>Last Name</th><th>Area Code</th><th>Phone #</th><th>Ext.</th><th>Area Code</th><th>Fax #</th><th>E-mail</th></tr>
<tr><td>Doc. prepared by</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>DIB Primary contact</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>ITB FSR contact</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Project Manager</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

2.3 Section C: Project Relevance to State and/or Departmental Plans

1.	What is the date of your current Operational Recovery Plan (ORP)?	**Date**	07/15/2005	**Project #**	**2004-01**	
2.	What is the date of your current Agency Information Management Strategy (AIMS)?	**Date**	01/2003	**Doc. Type**	**FSR**	
3.	For the proposed project, provide the page reference in your current AIMS and/or strategic business plan.	**Doc.**	ITB Strategic Plan			
		Page #	10 & 11			

		Yes	**No**
4.	Is the project reportable to control agencies?	✓	
	If YES, CHECK all that apply:		
✓	The project involves a budget action.		
	A new system development or acquisition that is specifically required by legislative mandate or is subject to special legislative review as specified in budget control language or other legislation.		
	The project involves the acquisition of microcomputer commodities and the agency does not have an approved Workgroup Computing Policy.		
✓	The estimated total development and acquisition cost exceeds the departmental cost threshold.		
	The project meets a condition previously imposed by Finance.		

2.4 Section D: Budget Information

Project #	2004-01
Doc. Type	FSR

Budget Augmentation Required?		
No		
Yes	✓	If YES, indicate fiscal year(s) and associated amount:

FY 06/07	FY 07/08	FY 08/09	FY 09/10	FY 10/11	FY 11/12
$ 1,758,779	$ 10,956,112	$ 12,632,247	$ 3,551,113	$ 3,295,073	$ 3,237,073

Project Costs

		06/07	07/08	08/09	09/10	10/11	11/12	Total
1.	Fiscal Year	06/07	07/08	08/09	09/10	10/11	11/12	Total
2.	One-Time Cost	1,758,779	10,956,112	12,016,703				24,731,595
3.	Continuing Costs			615,544	3,551,113	3,295,073	3,237,073	10,698,802
4.	TOTAL PROJECT BUDGET	$ 1,758,779	$ 10,956,112	$ 12,632,247	$ 3,551,113	$ 3,295,073	$ 3,237,073	$ 35,430,397

Project #	2004-01
Doc. Type	FSR

Sources of Funding

		FY 06/07	FY 07/08	FY 08/09	FY 09/10	FY 10/11	FY 11/12	Total
5.	General Fund							$
6.	Redirection							$
7.	Reimbursements							$
8.	Federal Funds							$
9.	Special Funds	$ 1,758,779	$ 10,956,112	$ 12,632,247	$ 3,551,113	$ 3,295,073	$ 3,237,073	$ 35,430,397
10.	Grant Funds							
11.	Other Funds							
12.	PROJECT BUDGET	$ 1,758,779	$ 10,956,112	$ 12,632,247	$ 3,551,113	$ 3,295,073	$ 3,237,073	$ 35,430,397

Project Financial Benefits

					FY 09/10	FY 10/11	FY 11/12	Total
13.	Cost Savings/Avoidances				$ 3,535,803	$ 4,796,046	$ 3,799,065	$ 12,130,914
14.	Revenue Increase							

Note: The totals in Item 4 and Item 12 must have the same cost estimate.

2.5 Section E: Vendor Project Budget

Project #	2004-01
Doc. Type	FSR

Vendor Cost for FSR Development (if applicable) $ 292,495.00*

  Vendor Name: Eskel Porter Consulting

* Includes HIPAA Gap Analysis

Vendor Project Budget

1.	Fiscal Year	FY 06-07	FY 07-08	FY 08-09	FY 09-10	FY 10-11	FY 11-12	TOTAL
2.	Primary Vendor Budget*		$ 4,282,500	$ 6,725,000				$11,007,500
3.	Independent Oversight Budget	$ 100,000	$ 120,000	$ 120,000				$340,000
4.	IV&V Budget	$ 500,000	$ 1,000,000	$ 1,000,000				$2,500,000
5.	Other Budget	$ 400,000	$ 268,750	$ 218,750				$887,500
6.	TOTAL VENDOR BUDGET	$ 1,000,000	$ 5,671,250	$ 8,063,750				$14,735,000

Project #	2004-01
Doc. Type	FSR

---(Applies to SPR only)---

Primary Vendor History Specific to this Project

7.	Primary Vendor	N/A
8.	Contract Start Date	
9.	Contract End Date (projected)	
10.	Amount	$

Primary Vendor Contacts

	Vendor	First Name	Last Name	Area Code	Phone #	Ext.	Area Code	Fax #	E-mail
11.	N/A								
12.									
13.									

2.6 Section F: Risk Assessment Information

Project #	**2004-01**
Doc. Type	**FSR**

Risk Assessment

	Yes	No
Has a Risk Management Plan been developed for this project?	✓	

General Comment(s)
The Risk Management Plan is included in Section 7 of the FSR.

3.0 BUSINESS CASE

Business practices surrounding HIPAA compliance have impacted the Employment Development Department (EDD), Disability Insurance Branch (DIB). This FSR section summarizes EDD organizations, programs, and processes. It describes DIB's business problems and opportunities, and sets objectives to address them in the following sub-sections:

>   3.1   Business Program Background
>
>   3.2   Business Problem or Opportunity
>
>   3.3   Business Objectives
>
>   3.4   Business Functional Requirements

3.1 Business Program Background

3.1.1 Employment Development Department Programs

The EDD administers the Job Service, Unemployment Insurance, Disability Insurance, and Workforce Investment Act programs for the State of California. As California's largest tax collection agency, EDD also handles the audit and collection of employment taxes and maintains employment records for more than 19 million California workers. One of the largest State departments, EDD has approximately 10,000 employees located at hundreds of service locations, providing many important services including:

- Assisting California employers in meeting their labor needs

- Helping California job seekers obtain employment

- Administering the federally-funded workforce investment programs for adults, dislocated workers, and youth

- Assisting disadvantaged citizens to become self-sufficient

- Helping unemployed workers by administering the Unemployment Insurance (UI) program

- Helping disabled workers by administering the Disability Insurance (DI) program

- Supporting State activities and benefit programs by collecting and administering employment-related taxes (UI, DI, Employment Training Tax, and Personal Income Tax withholding)

- Providing comprehensive labor market information

Along with the Department of Industrial Relations, the Agricultural Labor Relations Board, and the California Workforce Investment Board, EDD operates as part of the Labor and Workforce Development Agency. The EDD delivers programs that contribute to the economic development and security of California. As a public organization, EDD seeks opportunities to improve service delivery and customer service through partnerships with other public and private entities.

The EDD entities include:

- **Directorate**—Determines the direction of the department to ensure that programs and services are consistent with the department's mission and goals.

- **Administration Branch**—Provides administrative support to the department, including providing business operations planning and support services; human resource services; and accounting for the department's annual budget of more than $11 billion for fiscal year 2005-2006.

- **Disability Insurance Branch**—Provides temporary partial wage replacement for California workers who are unable to work due to illness, injury, or pregnancy. It is a State-mandated plan and allows for employer-administered voluntary plans. The DIB also administers the non-industrial DI program for State employees, the DI Elective Coverage program for self-employed individuals, and the Paid Family Leave program.

- **Information Security Office**—Responsible for enterprise security for EDD programs, services, and data. Delineates security policies, mechanisms, and processes in support of EDD operations.

- **Information Technology Branch**—Responsible for automation planning, policy, development, maintenance, support, operations, and oversight of automation and telecommunications systems within the department.

- **Job Service Branch**—Offers services at more than 400 locations statewide and connects 1 million job seekers with employers each year.

- **Legislative Liaison Office**—Serves as the department's primary liaison with the legislature, and develops analysis on legislation impacting EDD.

- **Program Review Branch**—Performs review, oversight, and technical assistance functions for the Director, EDD's Executive Staff, and State and local EDD program managers.

- **Public Affairs Branch**—Provides outreach, marketing services, communications, and training that support EDD programs and the employment of special targeted populations.

- **Tax Branch**—Handles all administrative, education, customer service, and enforcement functions for the audit and collection of UI, DI, Employment Training Tax, and Personal Income Tax (PIT) withholding.

- **Unemployment Insurance Branch**—Provides and accounts for program benefits to individuals who have lost their jobs through no fault of their own, are actively seeking work, are able to work, and willing to accept employment. For SFY 04/05, EDD will pay out more than $4.8 billion in UI benefits and receive and process more than 2.4 million new claims.[1]

- **Workforce Development Branch**—Administers several statewide workforce preparation programs and initiatives that focus on preparing adults and youth for participation into the labor force and building the State's economy.

---

[1] Amounts are actual through March 2005, and estimated for the remainder of the fiscal year.

The focus of this FSR is the Disability Insurance Branch, which administers California's State Disability Insurance (SDI) program.

3.1.2 DI Branch Program Description

The stated mission of the DI program is to "minimize the financial hardships for eligible disabled workers by providing timely and affordable benefits and services while supporting California's economic stability." Its corresponding strategic vision is that "California's State Disability Insurance Branch will be a leader and model for excellence, innovation, integrity, and commitment to customer service"[2]

To meet its mission and strategic vision, the DI program provides temporary, partial wage replacement to eligible disabled workers of California who suffer a loss of wages when they are unable to work due to illness or injury. The program was originally established in 1946 to provide economic protection to workers not covered by Unemployment Insurance and Workers' Compensation. Only four other states and one Commonwealth (Rhode Island, New Jersey, New York and Hawaii, and the Commonwealth of Puerto Rico) offer a state administered disability insurance program. Only Rhode Island and New Jersey are similar to California.

State disability insurance benefits are paid to qualified individuals who are unable to perform their regular or customary work due to mental or physical illness or injury, as well as pregnancy and childbirth. Additionally, DIB administers the Paid Family Leave (PFL) and the Non-Industrial Disability Insurance (NDI) programs. The EDD is required to promptly pay or deny benefits. Benefits are payable for a maximum of 52 weeks. In SFY 04/05, DI staff will process more than 700,000 initial claims and pay DI benefits paid to disabled workers totaling $3.2 billion. The DI program administration budget for the same year will total $237 million.[3]

The DI program is completely funded through employee payroll deductions. For 2005, employees in the State of California pay 1.08% of their taxable wages (subject to a dollar limit ceiling of $79,418) to the State Disability Fund. The DI program covers the majority of California employees, approximately 12 million workers, although some employees are exempt from DI. For example, railroad employees, employees of non-profit agencies, employees who claim religious exemptions, and most government employees are exempt from DI.

3.1.2.1 DI Plans and Benefit Programs

The DIB administers multiple insurance plans, each with different parameters and eligibility requirements. Mandatory DI and PFL coverage is provided through the State Plan or an EDD-approved Voluntary Plan (VP). DI covers State employees. Private employers and self-employed individuals who are not required to have DI coverage may participate in the DI Elective Coverage (DIEC) Program. The Non-Industrial Disability Insurance (NDI) Program provides a wage continuation benefit for State employees. Plans include:

- **State Plan—**This plan covers the majority of employees in California. Individuals not subject to the California Unemployment Insurance Code may also elect coverage at the

---

[2] Source: Disability Insurance Branch Strategic Plan 2002-2005.

[3] Amounts are actual through March 2005, and estimated for the remainder of the 04/05 fiscal year. Does not include AS&T, CUIAB Shares, and PFL statistics.

same rate as employees covered by the State Plan and with the same benefits as the State Plan.

- **Voluntary Plan**—This private plan may be substituted for the State Plan, once approved by the Director of EDD. Employers and employee groups may establish Voluntary Plans if the majority of employees and the employer agree to do so.

Benefit programs include:

- **The DI Elective Coverage (DIEC) Program**—Administered by DIB, DIEC provides benefits to eligible business owners and self-employed individuals suffering a loss of income when they are unable to perform their usual work due to illness, injury, or pregnancy. DIEC premiums are based on net profit reported on Internal Revenue Schedule SE. The maximum weekly benefit rate is the same as the DI program, and benefits are payable for a maximum of 39 weeks.

- **Non-Industrial DI (NDI) Program**—The DIB administers the NDI program for the Department of Personnel Administration (DPA). It is a short-term taxable wage continuation program for injuries, illnesses, and pregnancy. The NDI program provides benefits for State employees who are active members of the Public Employees Retirement System or the State Teachers' Retirement Systems; and for State Officers or employees of the Legislature. The maximum weekly benefit is determined by the employee's bargaining unit, and benefits are payable for a maximum of 182 days.

- **Paid Family Leave (PFL) Program**—The PFL benefits are administered by DIB and voluntary plans as are SDI benefits, and are funded by employee contributions as well. The PFL benefits are provided for up to six weeks, in a 12-month period, to persons who need to be off work to care for a seriously ill family member or to bond with a new child. The PFL program was recently implemented using the same basic approach and some of the same technology proposed in this FSR for administering SDI benefits.

3.1.2.2 DI Branch Organization

The DIB is comprised of the Senior and Administrative Offices, Central Office, and DI Field Offices (FOs). The Deputy Director and Assistant Deputy Director of the Disability Insurance Branch answer to the EDD Directorate. The Senior Management Team (SMT) is comprised of the Deputy Director, Assistant Deputy Director, Field Operations Division Chief, Paid Family Leave Project Manager, Section Managers, and the Deputy Director's Unit Manager. The SMT develops policy, sets program direction, and collaborates with business partners at an enterprise level. The Regional Managers report to the Field Operations Chief and provide DI field office oversight and administrative support. The DIB is organized as follows.

- **Medical Director's Office**—The Medical Director's Office provides guidance and support for EDD in the areas of reasonable accommodation and addresses employee health and safety issues. Specific to DIB, the Medical Director oversees the independent medical examination (IME) process, the IME medical panel, and provides medical guidance and training to DI claims examiners.

- **DI Central Office (DICO)**—The DICO provides operational support to DIB. DICO staff members analyze and develop legislation and regulations; develop and disseminate policies and procedures; develop and provide training; provide budget, personnel and facility direction and support; provide PC workstation and Single Client Data Base

(SCDB) system support and provide liaison and coordination with other EDD programs and support entities.

- **The DI Field Offices (DIFO)**—The DIFOs are comprised of Claim Management Offices (CMOs) and Customer Service Centers (CSCs). Field Office staff conduct day-to-day operational activities and are responsible for claim management and for providing secure, accurate, and timely information to workers, employers, and medical providers.

- **Claim Management Offices (CMO)**—The CMOs process claims, determine eligibility, and manage claim duration and workload. The CMO staff represents EDD at the Office of Appeals and the Workers' Compensation Appeals Boards (WCAB). The CMOs are located throughout the State.

- **Customer Service Centers (CSC)**—The CSCs provide customer service while managing incoming customer telephone inquiries. The CSCs answer information calls on EDD services and DI program information and specific claim-related calls and are located in Sacramento and Riverside. Prior to 1998, 22 field offices paid or denied initial claims and handled customer service inquiries for their administrative areas. To increase efficiency and improve customer service, the DI envisioned and implemented a central intake facility model. The first CSC began handling customer service inquiries for Northern California offices in 1998; a second CSC was implemented in early 2000. A toll-free telephone number for all customer inquiries statewide was implemented in 2000. All claim-related phone calls were redirected to the CSCs in 2004. There are currently 193 Disability Insurance Program Representatives (DIPRs) answering telephone calls in two CSCs. There are now 17 CMOs in addition to the CSCs.

3.1.2.3 DI External Customers

The DI external customers include any person, group, or organization that seeks DIB's attention, benefits, or services. The nine primary DI program external customers are:

- **Ratepayers**—California's approximately 12 million workers want the DI contribution rate kept as low as possible, to keep their personal costs low and the DI fund solvent so that full benefits will be available to them if they are needed.

- **Claimants**—As a subset of ratepayers, claimants are in immediate need of benefits and services. When claimants file their DI claims, they expect DI to process and pay their claims accurately and promptly. When they need to contact DI offices for assistance, they expect DI to respond to their questions and resolve their problems.

- **Medical Providers**—Medical providers certify claimants' medical eligibility for DI, estimate the duration of eligibility, and provide essential information to DIB. They perform a vital service for the DI program that significantly impacts benefit costs. Medical providers desire a program that operates efficiently for their patients, requires them to complete minimal paperwork and inquiries for DI, and thus reduces their cost of participation.

- **Employers**—Employers provide information on the DI Program to their employees. When their employees file a DI claim, employers provide employment and wage loss information to the DI Program.

- **California State Employees Association (CSEA)**—The CSEA represents DI employees. The DIB works with union representatives to ensure that employee

perspectives are heard and DI processes are conveyed and understood. The CSEA desires a healthy, safe, respectful, and supportive work environment for staff.

- **California Legislature**—The Legislature, through legislation and the State budgeting processes, can significantly impact DI program requirements, operations, and funding levels. Individual legislator contacts with claimants affect their attitudes toward the DI program. The Legislature desires that the DI program provide timely and affordable benefits and services to the people of California.

- **California Office of Appeals**—Administrative Law Judges (ALJs) conduct appeal hearings regarding UI and DI claims. When the ALJs decision is disputed, the aggrieved party has the right to appeal to the second-level appeals board. The COA desires that the DI program process and refer appeals timely and accurately, and provide knowledgeable representatives at hearings.

- **Workers' Compensation Appeals Board (WCAB)**—The WCAB has jurisdiction over Workers' Compensation (WC) liability disputes between employees and employers. It also acts as an appeals board to further resolve disputes. The WCAB desires that EDD representatives be knowledgeable, available, and have the authority to resolve EDD liens equitably and expeditiously.

- **Voluntary Plan (VP) Administrators and Employers**—VP Administrators administer approximately half of all VPs. Employers self-administer the others. In order to pay their claimants in a timely fashion, VP Administrators and employers need prompt responses and accurate information from DI.

3.1.3 DI Business Process Description

Figure 3-1 illustrates the primary DI business functions in the sequence the functions are performed. These functions are described briefly in this FSR section. Additional information is found in FSR Section 4, Baseline Analysis.

Figure 3-1. DI Branch High-Level Business Functions
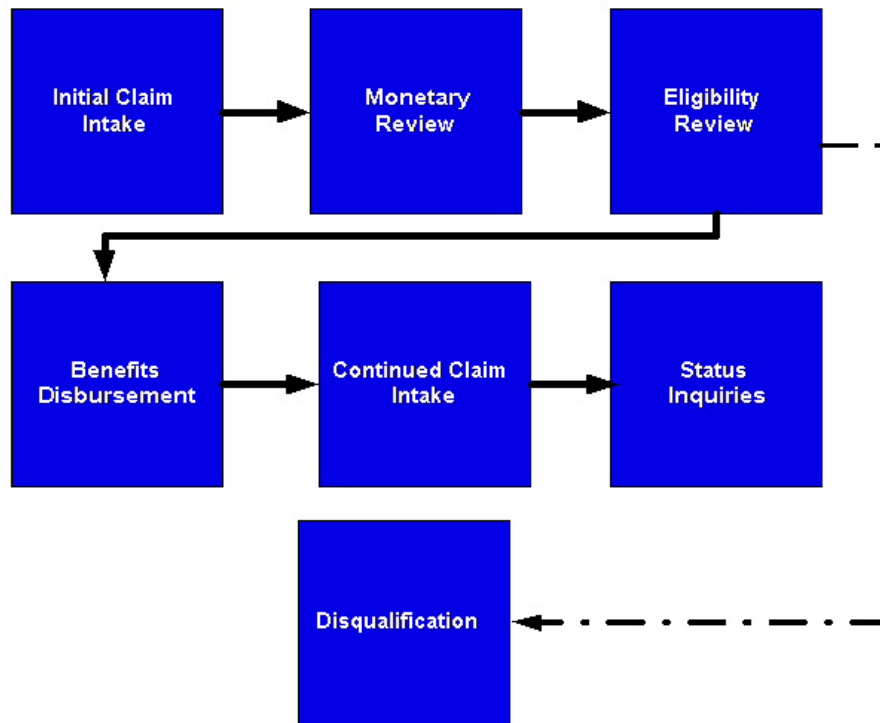
The claims process begins when an injured, ill, or pregnant person obtains a claim form and submits it. The EDD/DI provides a standard form, the Claim for State Disability Insurance Benefits, DE2501, for claimants to use to apply for DI State Plan and elective coverage benefits. This form may be obtained from medical providers, employers, and DI offices. The claim forms can also be obtained from EDD via:

- Telephone

- Voice mail/answering machine request line

- Written request

- In-person request

- E-mail request through the EDD's Web page

- Printing the form from EDD's Web page

3.1.3.1 Initial Claim Intake

A DI claimant obtains a claim form from a medical provider, an employer, or EDD and then fills in the claimant portion of the form. Claimants are responsible for getting the appropriate medical provider to fill out the portion of the form that verifies the existence of and the severity of the claimant's disability. The medical provider completes the required doctor's certificate portion of the initial claim form and submits it to DI or returns it to the claimant who then submits it to DI.

Most medical providers consider the procedure costly and burdensome and some medical providers even charge the claimant for the time involved in filling out the claim form. It should

be noted that there is no State law or regulation that requires medical providers to provide claimants or DI with this requested health certification information.

If claimants do not understand the instructions provided on the claim form, or have program questions, they may contact the DI CSC office by telephone, in writing, or look up the information on the EDD Web site.

Once a completed form is received at one of DIB's 17 claims management offices, DI clerical staff and claims examiners manually categorize the claim forms, review them for completeness, key the information into the DI mainframe computer system, and begin the initial processing tasks. After the intake process is completed, DI Field Office personnel retain information for their correspondence filing system where hardcopy documents and initial claim forms are stored.

3.1.3.2 Monetary Review

As part of the initial claims review process, a DI claims examiner conducts a monetary review of the claim using the mainframe DI system. The DI system uses EDD's Single Client Database (SCDB) master system, which supports the Tax and Unemployment Insurance Branches as well as DIB. The system automatically sends a form to the claimant's employer to report the receipt of the DI claim. The claims examiner validates the stated wages and status of other DI or UI claims.

3.1.3.3 Eligibility Review

The claims examiner researches the claim to ensure that the claimant is eligible for DI benefits. There are a number of disqualifying criteria for a claim, including, but not limited to, receipt of benefits from another source such as Unemployment Insurance or Workers' Compensation, and untimely claim filing. If there are eligibility issues that can be rectified, the examiner either resolves the issue or notifies the claimant of the issue in an attempt to resolve it. Denied claims can be appealed by the claimant and are adjudicated by the California Unemployment Insurance Appeals Board through a local Office of Appeals.

3.1.3.4 Benefits Disbursement

If the claim is monetarily eligible and meets program eligibility criteria, the benefit payments are calculated and the benefits disbursement process begins. Qualified claims are processed by SCDB and benefit payments are automatically printed and sent to claimants based on the computation of benefits. Back-end accounting systems are updated to reflect the benefit disbursement and claim documentation is filed.

3.1.3.5 Continued Claim Intake

A continued claim is a certification submitted by the claimant after the initial qualified claim has been paid. If a claim is longer than 6 weeks of benefits, the DI claim will go into automatic payments. Approximately 60% of DI claims go into automatic payment and claimants are not required to submit a continued claim form. Claimants who do not meet the criteria for automatic payments must re-certify their disability status every 2 weeks to continue to receive benefits. When a continued claim certification is received, clerical staff determine whether or not an examiner needs to review the claim for eligibility issues or whether the claim can be continued

as is. Once this decision has been made, the continued claims process includes online entry of the information into the SCDB.

3.1.3.6 Status Inquiries

Claimants may call DIB's Customer Service Centers (CSCs) to receive claim status, payment history, eligibility information, employee contribution rate, and other general program and claimant-specific information. Claimants are provided with a personal identification number (PIN) for access to the Interactive Voice Response (IVR) system. Claimants may use the IVR system or speak with a CSC representative.

3.1.4 Impact of the Proposal on DIB's Business Processes

The following paragraphs describe how the implementation of the proposed automation project will impact DIB's primary business functions noted in the basic work flow chart in Figure 3-1.

3.1.4.1 Claim Intake

The proposed solution described in this FSR will improve claims submission processes by providing easier ways for claimants, medical providers, and employers to interact with DIB. Medical providers will be able to directly interface with DIB. Intelligent forms will give claimants, small medical providers, and employers more efficient access to DIB. If the claimant's medical provider has an electronic interface to the new DI system, the claimant will not have to go to the medical provider to seek written validation; the validation can occur through the direct interface process. Incoming paper claims will be converted to electronic media via image scanning and optical character recognition (OCR) technologies. With validations and user prompts built into the electronic claim forms, incomplete forms will become a rare occurrence.

New applications will match claim information received through different intake methods. Upon receipt of necessary claim information, the new system will interact with the existing SCDB systems to issue payments. If requested by the claimant, medical provider, or employer, non-mainframe forms may be sent electronically. The new system will maintain claims examiner notes and record changes.

Once all new intake methods are implemented, the solution will provide access to complete claim information electronically, eliminating the need to refer to paper documents. The DIB can electronically transmit workload to claims examiners for processing, regardless of their physical location throughout the State. Hard copy documents will not have to be mailed to other DI locations. Claims Management Office (CMO) staff will no longer have to maintain a correspondence filing system where hardcopy documents and initial claim forms are stored.

3.1.4.2 Monetary Review

Although monetary review is included in DIB's existing automated system, the proposed solution will automate additional routine functions. New applications will verify the accuracy of the associated wage credits upon which the benefit entitlement is determined, and flag potentially erroneous wage credits. The solution will compare the claim with prior DI and UI claims that may affect eligibility for benefits.

Additionally, claims examiners will have access to entire electronic files containing claims information. Examiners will have the capability to electronically communicate with claimants' employers to report receipt of claims. Employers can review forms online if there are any monetary review issues to resolve.

3.1.4.3 Eligibility Review

The proposed solution will automate a number of routine research processes to ensure that the claimant is eligible for DI benefits. This automation will include generating electronic queries to the Workers' Compensation Insurance System (WCIS) to determine if the claimant is also receiving benefits from that system during the same time period. The system will cue the examiner to potential cases of fraud by checking the document against known fraud characteristics. If there are eligibility issues that can be rectified, the claims examiner can electronically notify the claimant of the issue in an attempt to resolve it. In the event of appeals, the entire claim file can be either printed out or made available electronically to the California Unemployment Insurance Office of Appeals and WCAB for adjudication purposes.

3.1.4.4 Benefits Disbursement

The proposed solution will include new case management functionality to store, track, recall, and review financial information more effectively. Increased flexibility in accounting will include automatic update of claimants' records to reflect the benefit disbursement and assist in detection of potential fraud. All claim documentation will be filed in an electronic correspondence file. However, actual benefit payment will be a function of the legacy system.

3.1.4.5 Continued Claim Intake

Claimants will have more ways to submit continued claims electronically via the Internet. Hard copy continued claims will be scanned. When the continued claim certification is received, automated triggers and built in business logic will determine whether a claims examiner needs to review the claim for eligibility issues or whether the claim can be continued as-is. This will limit the need for clerical and examiner staff to exception processing only.

The automated process will also enhance the current SCDB autopay function. Once an automated determination has been made, the continued claims process will not require any further online key data entry of the information into the SCDB. With this functionality in place, only rejected continued claims will require any processing intervention by DIB claims staff.

3.1.4.6 Status Inquiries

Currently, claimants may call Customer Service Centers to obtain information on claim status, payment history, eligibility information, employee contribution rate, and other general program and claimant-specific information. With the proposed solution in place, staff members (with security rights and privileges) will have access to the entire electronic case management file and will be able to answer questions and respond to claimant inquiries more efficiently, thus providing a higher level of service to claimants. Since all claim data will be stored electronically, future development may include an "online" claims status application to assist in serving claimants.

Internal to the department, the proposed solution will impact the EDD's Information Technology Branch, the UI Branch's Insurance Accounting Division, the Program Review Branch, The Information Security Office, the Investigations Division, the Audit and Evaluation Division, the Tax Branch, the Administration Branch, the Fiscal Programs Division, and the Office of Documents, Publication and Distribution—all who receive, provide, or share data with DIB. With more information available electronically, these units will receive more DIB-related information that will provide them with better decision-making capability. Moreover, any additional hardware, software, or infrastructure components will require support from ITB. Other State agencies that share data with the DI program will continue with no negative impacts.

3.1.5 Customers and Users

Table 3-1 provides a list of EDD's major customer and user groups, including a brief description of their current relationship with DI.

Table 3-1. Customers and Users

Customer Group	Relationship
Claimants	Claimants file for DI benefits for their own illness or injury.
Medical Providers	Certify medical information for all claims.
Employers	Verify information provided by claimant regarding employment, such as payment of leave, Workers' Compensation claims, and last date worked.
Department of Industrial Relations & Department of Workers' Compensation	Exchanges information with DI regarding Workers' Compensation claims, resolves liens, and works with DIB to combat fraud.
California Unemployment Insurance Appeals Board Office of Appeals	Hears 1st level appeals for all claims.

User Group	Relationship
Disability Insurance Workforce	Responsible for DI claims processing, key data input of information into automated system, determination of eligibility, case management activities, accounting and disbursement activities, all customer service activities, and all other processes that must be executed in support of DI.
DIB Program Management	Generates, receives, and analyzes management and operational reports to uncover trends, patterns, inefficiencies, fraud, and other information that will assist in improving the program.
Information Technology Branch	Provides technical project management assistance, design, development, maintenance, and operational support for DI automated and telecommunication services.

User Group	Relationship
Unemployment Insurance Branch- **Insurance Accounting Division** **UI Claims Overpayment Workforce**	Investigates and makes determinations for claims involving overlapping DI and UI benefits. Receives information for all DI claims in order to provide general ledger functions and other accounting services supporting the distribution of benefits. Re-computes DI benefit calculations. Responsible to account for UI and DI overpayment accounts.
Program Review Branch- **Compliance Review Division** **Investigations Division** **Audit and Evaluation Division**	Conducts programmatic audits/case reviews. Investigates and coordinates prosecution of identified DI fraud. Conducts DI administrative audits.
Tax Branch	Handles tax collection and withholding for DI, UI, and payroll taxes. Responsible for collection of UI and DI overpayments.
Administration Branch- **Fiscal Programs Division** **Office of Documents Publications and Distributions**	Provides program claim filing estimates and calculates the DI contribution rate. Provides program fund and workload forecast, budget and accounting functions, human resource services, and business services. Performs form composition and management, distributes over 150 hardcopy DI forms, receives data from IT, and prints and distributes DI benefit checks and over 200 different DI SCDB forms in an Automated Document Factory.
Information Security Office	Provides security oversight and risk management to DIB. Ensures the integrity and security of EDD information assets. Establishes and enforces policies and procedures to protect and secure IT infrastructure.

3.2 Business Problem or Opportunity

Although EDD is not formally required to comply with the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), the law significantly impacts DIB. This section of the FSR contains background information about HIPAA and explains the HIPAA-related challenges facing DIB.

HIPAA is comprised of the following two components:

- Title I, Health Care Access, Portability, and Renewability—protects health insurance coverage for workers and their families when they change or lose their jobs.

- Title II, Preventing Health Care Fraud and Abuse; Administrative Simplification; and Medical Liability Reform—requires the federal Department of Health and Human Services (HHS) to implement a series of standards, regulations, and provisions that include:

  - Electronic health care transaction and code sets (final rule issued)

  - Health information privacy (final rule issued)

  - Security requirements (final rule issued)

  - Unique identifier for employers (final rule issued)

- Unique identifier for providers (proposed rule issued; final rule in development)

- Unique identifier for health plans (proposed rule in development)

- Enforcement procedures (interim rule issued; proposed rule in development)

HIPAA implements consistency and makes it easier for health plans, health care clearinghouses, doctors, hospitals and other medical providers (collectively called "covered entities") to process claims and other transactions electronically. The law places stringent requirements on covered entities that communicate patients' protected health information (PHI) through the adoption of privacy and security standards.

While DIB recognizes that it is not a covered entity under HIPAA, it *is* a key link in the "chain of trust"[4] that must be in place to protect sensitive health information. California law (Unemployment Insurance Code, Part 2, Chapter 2, §§ 2700-2714 et seq.) requires DIB to receive health information from HIPAA covered entities. Claimants must establish medical eligibility by having a duly licensed medical provider certify the authenticity of the claim.

Medical providers have implemented HIPAA standards for health-related data, including methods for exchanging and storing data electronically. Transacting business electronically is cost-efficient and has become the norm for medical providers. Furthermore, they follow rigorous HIPAA-compliant policies and procedures to meet their patient privacy and information security responsibilities. Medical providers expect the same HIPAA-compliant business practices from all links in their chains-of-trust, and are encouraging DIB to make improvements that are necessary to solidify their own HIPAA compliance.

In addition to making interactions with medical providers more efficient, improvements to DIB's systems and processes in support of compliance with HIPAA will accelerate DIB's efforts in improving services and reducing costs. Implementation of HIPAA regulations and guidelines will allow DIB to realize the benefits that are common to organizations providing services through Electronic-Government (E-Government or E-Gov).[5]

To that end, DIB initiated an effort to determine the steps necessary to comply with HIPAA, to simplify its administrative processes, to interact securely with medical providers, and to improve claimant access to services. The DIB contracted with Eskel Porter Consulting and teaming partner Hubbert Systems Consulting (EPC/HSC) to conduct a HIPAA gap analysis of DIB's systems and processes, identify solutions to meet DIB's goals, and prepare a Feasibility Study Report (FSR).

The focus of the gap analysis included these HIPAA regulations:

- Privacy Rule

- Security Rule

- Transaction and Code Sets (TCS)

---

[4] "Chain of trust" is a term used to describe secure identification systems as well as documented procedures used to protect electronically transmitted data in HIPAA regulations.

[5] "E-Gov" is a generic term for Web-based services from agencies of local, state and federal governments. Such Web sites provide a wide variety of services to the public and have been extremely helpful in reducing internal paperwork.

EDD Employment
Development
Department
State of California

DI Automation Project, Phase 3
Feasibility Study Report

In addition to these regulations, the gap analysis and FSR process compared DIB's systems and processes with HIPAA guidelines for administrative simplification, including:

- Efficiency through electronic communications

- Reduction of fraud and abuse

- Standardization of data

- Quality assurance mechanisms

EPC/HSC also identified DIB-specific objectives and process improvements that align with and are recommended for implementation in conjunction with HIPAA standards.

The HIPAA Gap Analysis Report, provided as FSR Appendix D, strongly recommends that DIB take proactive measures to mitigate its risks of HIPAA non-compliance, and identifies its key problems in meeting the three HIPAA regulation areas. In addition, the EPC/HSC team found that the current DI program data interchanges with HIPAA-covered entities are manual and inefficient, lack adequate information access control, and contribute to the risk of fraudulent activity.

The gap analysis study found that the current paper-based certification process is burdensome and costly to both the medical provider community and DIB. If DIB cannot accept PHI electronically in a secure manner, additional layers of manual processes must be added for privacy and security, markedly increasing the cost of doing business for both parties. The use of PHI in the processing of a DI claim is a key factor in certifying the claim and, as a result, protected information is referenced extensively throughout the entire DI claim process.

Although some HIPAA privacy requirements are already addressed in the DI program due to other related State and federal laws, most are not. If DIB does not address its HIPAA gaps, DIB faces consequences that are summarized in the following categories:

- **Medical provider-related**—If DIB is unable to accept electronic submission of certification data by its medical providers, both entities will continue to incur higher and higher costs associated with processing the manual documents. Additionally, because the medical provider community will have to resort to labor-intensive (non-automated) procedures, submission of the certification data may be delayed. Without receiving the required certification of health information in a timely manner, DIB would not be able to pay the benefits that are owed to its claimants in a timely manner. Lastly, without automation intervention, the current manual processes will continue to proliferate. The DIB will require a larger workforce to handle its workload, and the resultant workload and cost overhead put upon claimants, medical providers, and employers would continue to increase as well.

- **Claimant-related**—Without timely certified medical provider information, claimants will be required to wait longer periods to receive their benefits; the processing of claims would continue to be paper-based which is onerous and costly; and the claims process would be subject to a much higher level of abuse and fraud.

- **Cost-related**—The current paper-driven business processes are inefficient and expensive. If the current system continues, ratepayers will continue subsidizing an inefficient system with escalating operating costs. A larger and larger portion of the

insurance funds meant to assist the disabled will be diverted to administering the system.

- **Service-related**—The current system does not make it easy for claimants, medical providers, and employers to do business with DIB. Without a new solution, California State and EDD goals to be more responsive and more accountable will not be met. In addition, medical providers will pass along any costs they incur to the claimant, which will feed the current rise in medical costs.

- **IT-related**—The existing level of IT automation does not provide much flexibility. If new IT solutions are not implemented, manual processing will increase, along with the problems and costs inherent in such processes.

DIB's business problems and opportunities are outlined under the following headings:

3.2.1   Inability to Support Medical Providers' HIPAA Requirements

3.2.2   Few Choices for Access

3.2.3   Inefficient Systems and Processes

3.2.4   Program Integrity Concerns

3.2.5   Enterprise Benefits

3.2.1 Inability to Support Medical Providers' HIPAA Requirements

In the course of preparing this FSR, the HIPAA gap analysis revealed a number of problems related to DIB's support of medical providers' compliance in the three HIPAA regulation areas: Privacy, Security, and, Transaction and Code Sets (TCS); as well as Administrative Simplification guidelines. The HIPAA chain-of-trust support problems impact DIB itself, claimants, medical providers, and employers who do business with DIB. The HIPAA Gap Analysis Report in FSR Appendix D provides details. Summary information is provided in the following subsections.

3.2.1.1 HIPAA Privacy Regulations

Under the HIPAA Privacy Rule, health care providers, health plans, and health care clearinghouses are required to safeguard PHI in all forms, including paper documents, electronic records, and oral communications. The rule prohibits such organizations from using or disclosing PHI except as authorized by the patient, or as specifically permitted by HIPAA Privacy Regulations or other law. Furthermore, it extends compliance responsibility to organizations that are not covered entities themselves, but may perform covered business functions on behalf of a covered entity. Since the functions of DIB closely resemble those of a health plan, the gap analysis was performed as though DIB must meet HIPAA privacy requirements as a covered entity.

Each standard and implementation specification of the Privacy Rule has documentation that is required by covered entities in order to achieve HIPAA compliance. This documentation may include written policies, procedures, guidelines, processes, forms, or descriptions of decisions. The compliance documentation must be stored in easily retrievable formats (electronic and/or paper). The DIB's HIPAA privacy gaps are primarily the result of inadequate documentation, posing risks that include:

- **Medical providers' hesitation or refusal to share PHI.** Without additional HIPAA awareness (applicable policies and procedures) and privacy safeguard language in DIB documents, providers will be more reluctant to share PHI.

- **Inappropriate disclosure of PHI.** Implementing HIPAA privacy standards within DIB supports a higher level of protection of confidential information. Without these extra protections, DIB is at a higher risk of having confidential information used and disclosed inappropriately, whether intentionally or unintentionally.

- **Loss of PHI.** Physical and IT safeguards are needed to ensure that PHI is not intentionally or unintentionally misplaced, destroyed, lost, or applied incorrectly. Taking precautions based on HIPAA privacy standards will help prevent these occurrences.

3.2.1.2 HIPAA Security Regulations

The HIPAA Security Rule focuses on the secure creation, receipt, transmission, storage, and exchange of electronic protected health information (e-PHI). The rule assigns responsibility for e-PHI to the organization that has ownership of the data at any given point. As ownership of data passes from one organization to another, so does the responsibility for protecting it. Business processes and IT assets are involved in ensuring e-PHI security, including network infrastructure, systems, applications, and computing tools.

HIPAA security regulations are closely related to several requirements for HIPAA privacy compliance. In addition, they align with State security requirements defined in California's Information Protection Act (IPA), and are based on information security standards and practices that are common outside of HIPAA compliance.

The gap analysis for HIPAA security within DIB examined administrative procedures, physical security, technical security standards, and organizational standards. It was determined that DIB has successfully implemented many of the security safeguards required by HIPAA regulations. However, several safeguards have been partially addressed or have not been addressed to date. The DIB's HIPAA security gaps are characterized as follows:

- **Adherence to policies and procedures.** The security policies and procedures developed by EDD's ISO are appropriate, thorough, and capable of providing clear direction to staff. However, adherence to security policies and procedures is inconsistent and poses a significant vulnerability for DIB. In addition, external testing and security challenges are not performed with sufficient regularity. Such testing not only helps identify security flaws, but also improves familiarity with and use of security policies and procedures.

- **Network security enhancements.** The current safeguards provided for e-PHI while it is in transit or stored on the EDD network are inadequate and create an unacceptable level of risk.

- **Disaster recovery preparation.** Availability of e-PHI for DIB and others in EDD is dependent on current and comprehensive disaster recovery planning. Current disaster recovery assumptions regarding the resilience of data and recovery capabilities of facilities do not fully account for possible and likely threat scenarios.

- **Vulnerabilities with employees. The DIB** employees are reminded of their responsibilities to safeguard e-PHI through various methods, including signing appropriate forms. However, the importance of HIPAA compliance and financial

exposure to litigation justifies taking further steps that could include employee background checks and technological safeguards for access monitoring.

3.2.1.3 Transaction and Code Sets

If a HIPAA Transaction and Code Sets (TCS) standard exists for the data transacted by a covered entity, then it must be followed. For example, if a medical code set or identifier is utilized electronically during a HIPAA standard transaction, then the named HIPAA standards for the medical code set or identifier must be used. This concept was the underlying foundation used to examine DIB's HIPAA TCS compliance. The HIPAA TCS requirements fall into three categories:

- Transaction Standards—The majority of the HIPAA transaction standards do not apply since the HIPAA covered functions are not performed by DIB. The exceptions are the receipt of health care claims and the associated health care payment in the Independent Medical Evaluation (IME) claim submission and payment process. If DIB were a covered entity, it would be found out of compliance with these two transactions. To match the practices of medical providers, DIB should adopt the HIPAA transaction standards and implement electronic interfaces for data exchange.

- Medical Code Set Standards—The DIB currently uses HIPAA-standard International Classification of Diseases, 9th Edition (ICD-9) diagnosis codes and, therefore, no gap exists relative to medical code sets. However, DIB should remain attentive to best practices and pay close attention to valid ICD-9 codes, to ensure that obsolete ICD-9 codes are not used. Although the industry is currently moving toward an ICD-10 standard, HIPAA does not currently mandate this change. The conversion to ICD-10 is affecting both covered and non-covered entities throughout the health care industry. All organizations that store and use ICD-9 codes will need to be prepared to accept and use the new format, regardless of their HIPAA covered entity status. Procedure codes are included on the IME invoices (form DI 2546INV) for payment of independent medical evaluations. Currently, information from the independent medical evaluation is stored in the note fields of the SCDB, so there is no specific system processing of the procedure codes. DIAP3 will implement HIPAA standard procedure codes so that DIB and medical providers may exchange data in the same electronic formats.

- National Identifier Standards—Analysis specific to the two HIPAA National Identifier standards (Employer and National Provider) indicates a compliance gap. Multiple DIB systems capture a version of an employer or provider identifier, and that format meets the standard. However, the newly approved National Provider Identifier is in a format not used by DIB. Therefore, HIPAA TCS best practices recommend using the standard format, and medical providers will most likely convert to these new standards.

As a whole, the TCS gaps that were identified place DIB at risk of the following:

- **Strained relationships with medical providers and claimants.** Since medical providers expect to communicate with DIB in an electronic, HIPAA-compliant manner and DIB is unable to live up to that expectation, there may be increasing delays in exchanging data with medical providers. Medical providers' costs may increase to cover manual processes needed to interact with DIB. Added delays and expenses will have a negative impact on timely payments to DI claimants or no payments at all.

- **Continually increasing administrative costs.** Existing DI claims processing is labor intensive and exemplifies the inadequacies associated with significant human intervention. As the population of California increases, the submission of disability claims will also increase, along with the number of DIB staff required to process the claims. Employee expenses, as well as the cost associated with handling and storage of paper documents, will continue to raise administrative costs.

- **Unnecessary duplicative processing.** Medical providers' data elements are in a different format than what DIB currently stores. Without the necessary system modifications, DIB will be required to develop a method to manually store and translate these data elements.

3.2.1.4 Administrative Simplification

The DIB's business processes consist of many complex manual operations supported by decades old technology and applications. The HIPAA Gap Analysis concluded that these processes do not conform to HIPAA's objectives of administrative simplification. Since medical providers have already implemented HIPAA-compliant systems and processes, DIB has become the choke point in end-to-end DI claims processing. Claimants, medical providers, and employers are forced to use paper-based labor-intensive processes to interact with DIB, resulting in inefficiencies, as well as privacy and security risks all along the chain-of-trust.

HIPAA's Administrative Simplification guidelines offer DIB an opportunity to realize benefits by implementing and following recommendations such as:

- **Increase efficiency through electronic communication**. Manual health care data exchange is currently a time-consuming, laborious task. Having all health care organizations adopt uniform electronic claims streamlines the process and reduces time and expense.

- **Standardize data**. The standardization of data elements, identifiers, and code sets has built a health information network that gives medical providers ready access to the information they need, whenever and wherever they need it, to best care for patients. Standardized data offers better reporting for management and industry needs.

- **Improve quality assurance mechanisms**. The health care industry's compliance with HIPAA has fostered the emergence of improved mechanisms for quality measurement, monitoring, and control. Through uniform identifiers, organizations are able to track providers over time and across settings to analyze patterns in the quality of care. Administrative data can be more easily analyzed to determine at what level health care organizations are meeting the needs of claimants.

- **Reduce fraud and abuse**. There are many documented cases of fraud and abuse in the health insurance and health care industries. The use of a secure communications and operations environment to protect a patient's medical information as well as standardized electronic transactions make it difficult for fraudulent operators to carry on abuses. The assignment of unique identifiers curbs the fraudulent practice of billing for nonexistent claimants. Using standard datasets and codes, auditors can observe suspicious trends.

3.2.2 Few Choices for Access

The current system does not make it easy for claimants, medical providers, and employers to do business with DIB.

- **Claimants have no other alternative than filing paper-based claims with DIB.** The process is not user-friendly nor does it allow claimants with access to computers or the Internet to file more promptly. The paper-based process makes it difficult to ensure the security and privacy of claimants' personal data and PHI.

- **Medical provider access to DIB is entirely paper-based.** Providers must spend time filling out inefficient paper forms and then often have to resubmit the same data because the original form was not correctly filled out or was lost. This is both burdensome and costly to them. They are unable to utilize patient data already in their own automated systems or input DI data into their systems. Because it takes them out of their normal process of electronic interaction, some medical providers charge DI claimants a fee for filling out the required paperwork. As medical providers move to exclusively electronic transactions, they may not complete DI claims form certification in a timely manner and may pass on the expense to their own patients.

- **Employers have no other alternative than to receive claim information from DIB in paper format.** This is a very inefficient system that creates a cost overhead for some employers. Increasingly, employers, especially larger ones, keep track of more and more information related to their employees. Those who collect and track this data are forced to key this information into their own automated systems, which creates a labor overhead for them. Additionally, if DIB's paper-based information is at variance with information contained in the employer's databases, they usually run a report from their own automated systems and then enter this data onto more paper-based forms and re-submit it to the DIB, thus incurring more overhead expenses.

3.2.3 Inefficient Systems and Processes

Many of the shortcomings of DIB's current processes and systems revolve around numerous paper-based data collection processes that require manual and often duplicative data entry into the legacy DI automated systems.

As summarized in Figure 3-2, the majority of DIB information flows use manual and paper-based methods. Flows highlighted in green and bold italic indicate electronic process; while all others indicate manual, paper-based information flow processes.

Figure 3-2. The DIB Information Flows
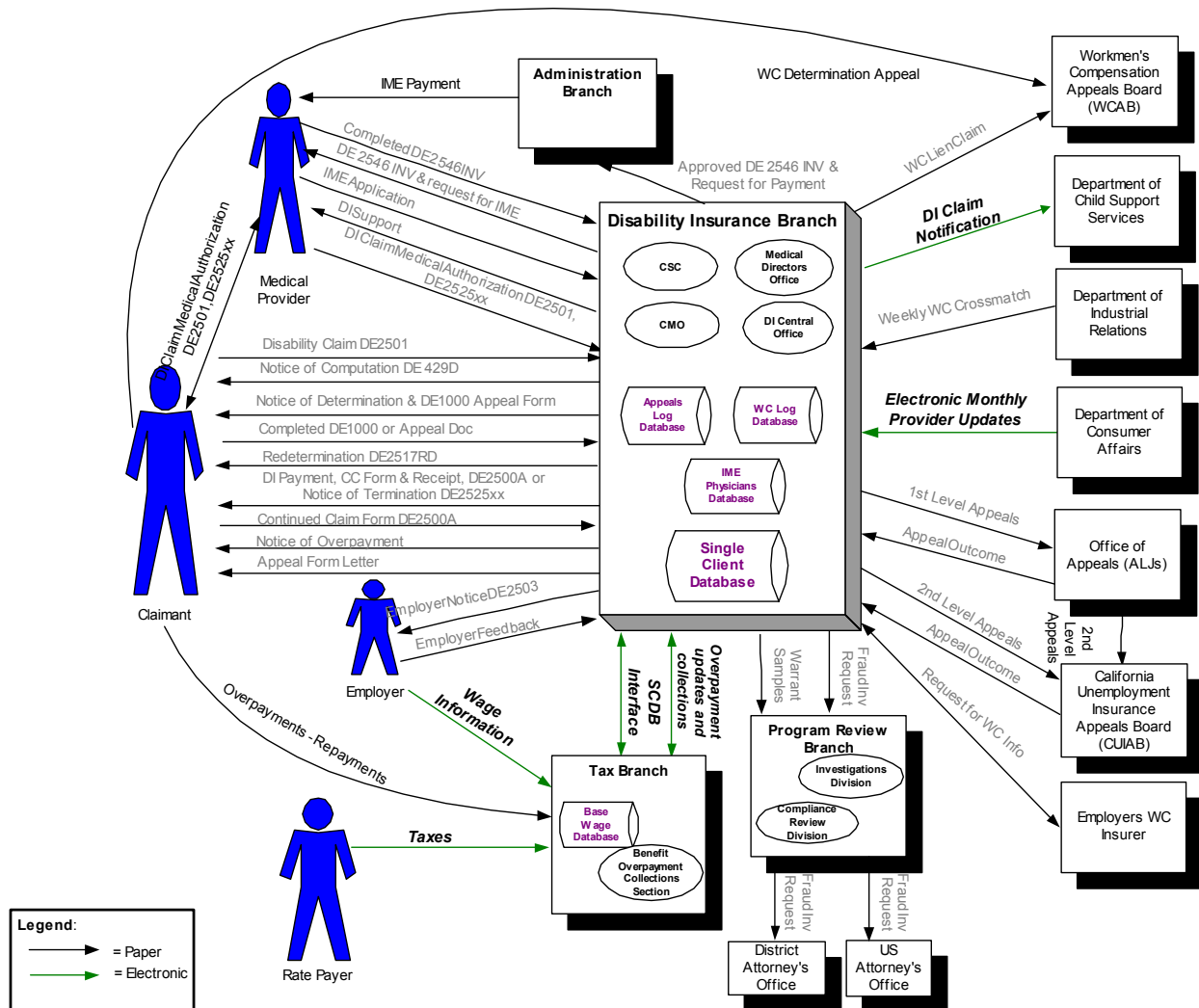
Additionally, DIB shares the SCDB database and some applications with the UI Branch, such as the Insurance Accounting Division's Automated Benefit Accounting System.

Process and system shortcomings include the following:

- **Current business processes can often be labor-intensive, time-consuming, paper-driven, serial processes.** Many of these processes involve redundant steps to ensure adequate claim information intake, and audit and control of customer-supplied data. Key data entry is a problem area both with regard to safeguarding sensitive HIPAA-covered information and operational cost efficiencies. The DIB response to customer or internal inquiries requires locating the hardcopy documents in question, which can take one or more days. Currently, hardcopy documents are stored, non-centrally, throughout the State. The sheer volume of incoming paper makes tracking and retrieval difficult. Also, the routing of hardcopy information increases the risk of exposure for health-related information, information loss and subsequent re-requesting, and the incidence of fraud.

Concurrent use of documents is not possible. Claim examiner processes are time-intensive because of the paper-based serial processes. Workload balancing among offices is accomplished by mailing paper claims.

The current reliance on Key Data Operators (KDOs) to manually input claim information into the DI system impacts backlog and payment in several ways. Backlog and payment delays result from incorrect keying of claim information, as well as from incorrect or illegible information provided by the claimant or medical provider. Once these errors are identified, the claim may need to be deleted from the system and re-keyed, disrupting timely claim processing and benefit payments. Additionally, each claim must be opened using a mail-opening machine, and at times, the mail-opener will slice/cut the claim form. The KDO must stop and repair the claim form before keying can take place. The current system does not allow for efficient centralized intake and distribution to locations where staff are available who have the capacity to take on the work. Instead, the paper claim forms are mailed to the DI office within a specific geographical area. For a variety of reasons, the location may lack the staff capacity to work the claims in a timely manner, resulting in backlogs and delays in payment. Backlogs and delays also result from claim forms being sent to the wrong geographic EDD DI Office. When a claim form is received at an incorrect location, the claim is placed in a mailer and mailed to the appropriate office. Furthermore, since there are no other options than to complete and submit paper claim forms by mail, there is always the opportunity for claim forms being lost of mutilated in the mail, resulting in the claimant having to resubmit the claim form.

- **Processes constrained by lack of advanced technology**. As a number of technical analyses of DIB's operations[6] have pointed out, many of DIB's processes have remained unchanged since the program's inception in 1946. Additionally, DIB's supporting IT architecture is heavily dependent upon decade's old technology[7] that limits DIB's ability to interact electronically among its 17 locations throughout the State, and with its claimants, partners, insurance and health communities, employers, and stakeholders. It also limits the organization's ability to implement additional automation, thereby creating more effective work processes. When compared to the capabilities of its medical provider business partners who have led the way in moving to electronic transmission-based processes, DIB's use of electronic transmission-based processes is significantly behind the technology curve.

  - **Process shortcomings**. The ability to address DIB's business process problems through automation illustrates another series of problems DIB faces. The DIB's supporting IT architecture is heavily dependent upon decades old technology and applications that limit the organization's ability to:

    - Minimize key data entry.

    - Effectively leverage data already in the automated system.

    - Further automate the handling of routine claims activity.

    - Automate the rejection of incomplete claims.

    - Automate the transfer of workload to other DI offices.

---

[6] Warner Group State DI Certification Process Re-engineering Project Report (May 1998), and KPMG's Review of Fraud Prevention, Detection, Deterrence and Investigation Activities Report (October 29, 2001).
[7] The SCDB is a mainframe-based application developed in Integrated Data Management System (IDMS) software which was developed by GE in the 1960s. The mainframe and software capabilities reflect 1980s technology capabilities.

– Provide integrity alerts to examiners in instances of possible fraud.

- **Inability to easily interface with modern systems.** Many of the shortcomings of the current system revolve around numerous paper-based data collection processes that require manual data entry into numerous legacy system screens. The EDD's and DIB's legacy systems cannot be easily modified to interface and communicate with systems which employ HIPAA-compliant electronic data interchange standards that allow secure electronic transfer of data between disparate systems. This limits DIB's ability to interact electronically with claimants, medical providers, and employers.

- **Technology shortcomings.** To administer data required for its mission-critical services, DIB utilizes several tightly coupled legacy mainframe systems, some of which are shared with other EDD programs. There are several problems relating to existing automated processes for DI claim processing – the legacy system is not amenable to provide either batch for real-time connectivity to data trading partners owing to production processing cycles and batch processing windows. The SCDB is supported on outdated database management technology and create a difficult and expensive connection from client server or web based systems. Support of the DI system and the SCDB is problematic in that the skills required are not readily available, making recruitment difficult, staff development is more expensive, and staff retention is exacerbated. The existing system is denying service to users in that the design is rigid, and its scale is very large, to the extent that making any change to the system design at a reasonable cost precludes the inclusion of new design features unless they are driven by unavoidable mandate. The legacy systems cannot:

  – Be modified quickly to comply with new statutory regulation and/or requirements

  – Be changed without concern for other program impact

  – Communicate seamlessly across the department and with their external partners

  – Add more business functionality into their systems and processes

  – Provide easy access to information needed for decision making

  – Easily leverage new technologies within EDD's enterprise

3.2.4 Program Integrity Concerns

Fraud and abuse are ongoing problems that DIB must combat. The situation was evaluated on several occasions, and is the subject of the *DI Fraud Prevention Detection, Deterrence, and Investigation Report* written by KPMG. One of the primary drivers for enacting HIPAA was to combat this concern and reduce waste in government. With the impetus of HIPAA compliance and following Administrative Simplification guidelines, DIB must resolve the following long-term program integrity problems:

- Manual methods for detecting fraud and abuse are often inefficient, ineffective, and labor intensive

- Assurance that patient health-related information is secure, private, and protected from fraud is lacking

- Rules for mitigating risk of fraud and losses to the DI fund are constantly being reevaluated, and many new methods have not been incorporated into the current automated system because it is difficult and expensive to modify

Although many of the fraud and abuse control provisions of HIPAA are related to Medicare and Medicaid, there are guidelines that may be adapted for incorporation into DIB's business model. For example, HIPAA created a program encouraging Medicare beneficiaries to report fraud and abuse and offer suggestions to improve efficiency of the Medicare program, and provides for payment to beneficiaries in certain cases. Additionally, standardized data makes detection of irregularities (and possible fraud) easier to automatically detect.

3.2.5 Enterprise Benefits

DIAP3 affords DIB the opportunity to align with EDD's strategic vision to leverage its IT investments to benefit the enterprise. The project moves DI claims processing away from paper. In addition to the inflated staff costs and privacy/security risks associated with processing paper, files at DIB's field offices are retained for 3 years, then transferred to a centralized warehouse for an additional 2 years prior to destruction, adding storage and transportation expenses.

If DIAP3 is not implemented, EDD must continue to face the challenges of handling and managing more than 6 million paper claim-related documents each year. The project's enterprise benefits include:

- **Using EDD-proven and easily integrated technologies.** The strategy and direction of DIAP3 aligns with EDD's IT strategies and initiatives. The project will employ stringent HIPAA-compliant security measures in alignment with EDD's Information Security Office. Since the SCDB system is expected to continue operations for the foreseeable future, EDD is implementing strategies intended to leverage its legacy systems. DIAP3 will utilize technologies compatible with or currently within EDD's technical environment, such as the Microsoft .NET Framework and messaging gateway software for interactions with legacy systems.

- **Establishing the Internet as a communication channel by employing electronic interfaces and Web-based intelligent forms.** Both the direct electronic interface and intelligent Web forms will reduce the number of paper claims submitted. Medical providers will be able to send electronic claims certification data directly to DIB through a secure interface. Intelligent forms will provide efficient, customer-centric methods of claim intake and processing. Intelligent forms edits will minimize follow-up inquiries, as missing or incomplete data will prevent submission of the claims. Application business rules will automatically issue disability payments if all requirements are met, and speed the payment process otherwise. Overall, the electronic interface and intelligent forms will increase customer satisfaction and reduce internal operational workload.

- **Using EDD's enterprise business model for IT support.** By adhering to EDD's enterprise IT support model, which leverages supported software tools and the skill sets of its technical personnel, the DI Automation Project Phase 3 can minimize IT support costs.

- **Using image scanning/OCR and document management solutions**. Although the electronic interface and intelligent forms will reduce DIB's paper claims volume, a need to process paper will remain. DIAP3 will leverage EDD's experience in using image scanning and optical character recognition (OCR) technologies, which are the cornerstone of the Tax Branch's Tax Engineering and Modernization (TEAM) project. Scanning/OCR reduced a very similar process involving data entry, paper handling, and

storage costs by approximately 45%. The DIB's PFL project also utilizes this technology. The DIB will use scanning/OCR and document management technologies to process paper claims. This technology will provide the added benefit of allowing DIB to electronically centralize its claims files and balance its workload among its field offices by sending/receiving files electronically.

3.3 Business Objectives

In his 2004 State of the State address, Governor Schwarzenegger said, "We cannot afford waste and fraud in any department or agency." These words are at the center of DIB's objectives for HIPAA compliance and automation. The DIB seeks to significantly improve on its delivery of services by focusing on five primary business goals, allowing the organization to:

- Improve access to services

- Improve service delivery

- Detect and prevent fraud and abuse

The DIB intends to undertake a business-based procurement to select a DIAP3 solution. Refer to Section 5 of the FSR for information regarding the potential solution. FSR Section 3.4.1 contains the general functional requirements that the selected solution must incorporate to satisfy the objectives related to each goal, as delineated in the sections that follow.

3.3.1 Improve Access to Services

The DIB Strategic Business Plan describes its goal of offering multiple communication methods to increase customer satisfaction. DIAP3 will implement HIPAA-compliant electronic communications through the direct e-interface and Web-based intelligent forms, creating two new intake channels to assist DIB in meeting its access objectives. Currently, 100% of claim transactions are paper-based. The DIB's objective is to obtain at least 70% of transactions (initial and continued claims, medical provider certifications) through electronic methods by the end of the first full year of DIAP3 operations. DIB will track this information through the solution's business intelligence/decision support function.

3.3.2 Improve Service Delivery

The DIB will overcome problems associated with manual, paper-based systems, thereby improving service delivery to its stakeholders. New intake methods will increase self-service options that allow claimants to be more responsible for providing DIB accurate and complete claim information through edits and business rules that promote accuracy and completeness of information received. Currently, human intervention is required for payment of claims. DIAP3 will allow DIB to meet its objective of having at least 50% of initial claim payments issued automatically, and achieving at least 20% of initial claim payments issued automatically by the end of the first year of operation. DIB will track this information through the solution's business intelligence/decision support function.

3.3.3 Detect and Prevent Fraud and Abuse

The DIAP3 solution will assist DIB in managing fraud and abuse through the implementation of HIPAA Administrative Simplification guidelines, including automated programs and business

logic to combat fraud. To combat fraudulent access, it will detect unauthorized access to PHI under EDD's ownership immediately upon implementation of the proposed solution, and automatically notify EDD's Audit and Evaluation Division (A&ED) and the ISO of all unauthorized access or attempted access to PHI. In its first year of operation, EDD will perform at least four periodic tests of the solution and will detect at least 80% of instances of fraud and abuse by simulated medical providers, employers, and claimants, as well as simulated unauthorized internal staff access.

Currently, DI relies on claim examiner discovery, hardcopy reports, and the DI Fraud Hotline to detect any fraudulent activities. The DIAP3 fraud component will use business intelligence and decision support technologies to detect fraud, such as creating claim profiling. This functionality will have the ability to flag claims for further review if they fit certain fraud parameters. The DIAP3 will also have the capability to track medical providers with a past history of fraud, allowing the DI Field Office Integrity Specialists (FOIS) to leverage existing fraud reports, and make notes in the system regarding the file. The new solution will also automatically select a random number of claims for quality control review.

3.4 Business Functional Requirements

The following DIB functional requirements were identified through HIPAA gap analyses, interviews with EDD and DIB, review of DIB's strategic plan, and from historical information. Upon approval of this FSR, DIB intends to use a business-based procurement approach to solicit solutions from vendors. As part of the business-based approach, DIB will contract with a procurement assistance vendor to solidify DIAP3 functional and technical requirements to the greatest extent possible without dictating a rigid solution. This will allow DIB to incorporate any additional HIPAA requirements that may have become final since submission of this FSR. It will also permit DIB to re-evaluate the impact of any EDD network or security infrastructure changes that may be in place at that time.

3.4.1 Goal 1—Improve Access to Services

3.4.1.1 Obtain at least 70% of transactions (initial and continued claims, medical provider certifications) electronically by the end of the first full year of operations.	• Define, develop, and implement direct interface with medical providers and other high-volume partners. • Implement Web-based intelligent forms for claims submission from claimants and small medical providers. • Uniquely identify all submissions. • Verify authenticity of all submissions. • Define and implement appropriate safeguards for external customer access. • Ability to access external electronic systems.[8] • Ability to ensure the integrity of communications with external customers. • Preserve confidentially and security of data. • Implement scanning/OCR to convert paper initial claim form, continued claim form, and medical provider certification form to electronic record. • Design, develop, and implement applications and database to augment legacy systems.	Compliance Reviews—160.308 Administrative Safeguards—160.308
3.4.1.2 Define the HIPAA Privacy requirements as applicable to EDD.	• Become compliant with applicable HIPAA privacy and confidentiality requirements. • Support HIPAA Privacy Rule as applicable to EDD. • Define, implement, and adhere to privacy policies, procedures, and forms. • Educate and provide HIPAA privacy training to DIB staff. • Establish and apply applicable HIPAA privacy claimant restrictions to disclosures. • Ensure all information classified sensitive or confidential is encrypted using minimum 128-bit key during data transport on all telecom and network systems. • Create an adequate level of documentation in order to demonstrate compliance with the HIPAA Privacy Rule and other applicable California law.	Compliance Reviews—160.308 Confidential Communications—164.502 Uses and disclosures of protected health information subject to an agreed-upon restriction—164.502 (c) Notice of privacy practices for protected health information—164.520 Training—164.530

---

[8] Reference Figure 4-13.

3.4.1.3 Define the HIPAA Security requirements as applicable to EDD.	• Implement an organization-wide Security Awareness Training and Education (SATE) program. • Ensure the SATE includes yearly updates for the entire workforce. • Implement safeguards that protect confidentiality, integrity and availability of PHI created, received, stored, or transmitted on behalf of a HIPAA-covered entity. • Employ technological safeguards for access monitoring. • Identify and respond to all real or suspected adverse events in relation to the security of DIB systems or networks. • Identify and respond to all real or suspected acts of violating an explicit or implied security policy. • Implement practices to comply with the IPA notification of breach requirements. • Define, implement, and adhere to all other HIPAA security requirements as applicable within EDD. • Define, implement, and adhere to HIPAA-compliant policies, procedures, and forms, as applicable. • Ensure all information classified sensitive or confidential is encrypted using minimum 128-bit key during data transport on all telecom and network systems. • Accept and submit appropriate ANSI X12 standard transactions in a secure electronic environment. • Ensure disaster recovery preparedness.	Security Standards—164.306 Administrative Safeguards—164.308 Assigned Security Responsibility—164.308(a)(2) Security Awareness and Training—164.308(a)(5)(i) Security Incident Procedures—164.308(a)(6)(i) Security Incident Response and Reporting—164.308(a)(6)(i) Evaluation—164.308(a)(8) Physical Safeguards—164.310 Facility Access Controls—164.310(a)(1) Person or Entity Authentication—164.312(d) Contingency Plan—164.308(a)(7)(i) *Information Practices Act—Civil Code §1798.29*
3.4.1.4 Define the HIPAA TCS requirements as applicable to EDD.	• Ensure that new applications and databases incorporate applicable HIPAA transaction standards. • Implement HIPAA transaction standards for IME claims and payments. • Review and update ICD-9 codes as needed. • Ensure flexibility in .NET application and SQL database to incorporate expected ICD-10 changes. • Implement electronic acceptance, access, and storage for medical codes.	Transaction and Code Sets 835: Health Care Payment and Remittance Advice 837: Health Care Claims or Equivalent Encounter Information *ICD-9- Clinical Modification CM, Vols. 1-3 Health Care Financing Administration Common Procedure Coding System, and Current Procedural Terminology, Fourth Edition (HCPCS & CPT-4)*

3.4.2 Goal 2—Improve Service Delivery

Objectives	Requirements	HIPAA *(or Other)* Reference
3.4.2.1 Issue at least 50% of initial claim payments automatically, and achieve at least 20% by the end of the first year of operation.	• Ability to authorize claimant, employer, agents of the State, voluntary plan, or medical providers access based on DI-defined criteria. • Ability for claimants, employers, voluntary plans, and medical providers to submit and access claim information via the Internet. • Improve ability for claimants, employers, voluntary plans, and medical providers to submit and access claim information via interactive voice response. • Design, develop, and implement direct interface with medical providers. • Implement intelligent forms for claims submission. • Implement edits and business rules to promote accuracy and completeness of information received. • Ability to create, implement and modify business rules to automate handling of routine claims activity, and process routine submissions and inquiries automatically. • Automate existing manual and update automated processes for claim intake, monetary review, eligibility determination, processing, and payment. • Accurately compute standard claim information (payments, offsets, etc.). • Integrate and update normal expected durations for disabilities in managing claims. • Define, implement, and update forms and edit and audit criteria for electronic submissions and inquiries. • Ability to generate management reports detailing payment activity. • Track and maintain medical provider information/status.	Administrative Requirements—164.308 Business Associates Contracts and Other Arrangements—164.308

Objectives	Requirements	HIPAA *(or Other)* Reference
3.4.2.1 (continued)	• Define and implement workflow with ability to identify available resources. • Compile and transmit all information relating to a claim. • Electronically shift workload to available resources. • Use workflow to track and monitor distributed work. • Provide electronic access claim and claim-related information. • Ability to manage claims/appeals as a "case" rather than individual forms. • Ability to process routine submissions/inquiries automatically. • Provide easy access to productivity tools. • Improve ability for claimants, employers, voluntary plans and medical providers to submit and access claim information via interactive voice response. • Provide standard and ad hoc reports.	Administrative Safeguards—164.308
3.4.2.2 Use existing technology assets.	• Utilize the SCDB platform, applicable functionality, and data repository. • Use messaging gateway to manage mainframe data updates, leveraging CICS screens and business rule logic. • Follow the .NET Framework. • Use EDD's enterprise business model for IT support, including supported tools and technical skill sets. • Use EDD's Information Security Office for HIPAA privacy and security services. • Leverage HHSDC hosting, infrastructure, and security services for intelligent forms servers and Internet access, including Tivoli Access Manager for e-business (TAMe).	Administrative Safeguards—164.308 Technical Safeguards—164.312

3.4.3 Goal 3—Detect and Prevent Fraud and Abuse

Objectives	Requirements	HIPAA *(or Other)* Reference
3.4.3.1 EDD will perform at least four periodic tests of the solution and will detect at least 80% of instances of fraud and abuse by simulated medical providers, employers, and claimants, as well as simulated unauthorized internal staff access.	• Ability to test the HIPAA chain-of-trust as simulated medical providers, employers, and claimants.9 • Ability to test the HIPAA chain-of-trust with simulated, unauthorized internal access. • Implement / improve quality assurance mechanisms. • Ensure that DIB employees understand and follow incident severity reporting requirements. • Detect unauthorized access to PHI under EDD's ownership immediately upon implementation of proposed solution. • Identify and automatically alert A&ED and ISO of inappropriate activity. • Authorize claimant, employer, agents of the State, voluntary plan, or medical providers access based on DI-defined criteria. • Identify, monitor, and address internal and external activity for patterns that indicate possibility of fraud. • Implement methods to regularly review assigned user roles and security privileges to control access to data. • Implement a comprehensive audit trail log for system security monitoring, analysis, review, investigation, and audit. • Create a new user interface with secure access to all relevant data sources. • Build logic into claim processing system that checks new claim data against data from claims already in the system in order to identify fraud indications (high number of claims with same name, address, SSN, doctor, etc.). • Maintain and improve business functions in support of Workers' Compensation.	Compliance Reviews—160.308 Administrative Safeguards—164.308 Technical Safeguards—164.312

---

[9] Reference Figure 4-13.

3.4.3.1 (continued)	• Ability to uniquely identify claims. • Ability to uniquely identify individuals. • Assign claims randomly to claims examiners (rather than by SSN). • Ability to identify previous fraudulent activity by claimant, employer, voluntary plan, or medical provider. • Ability to authorize claimant, employer, agents of the State, voluntary plan, or medical providers access based on DI-defined criteria. • Ability to analyze claim data to determine irregularities, trends and patterns; ability to view a digital "dashboard" for quick review of key fraud indicators. • Ability to automatically stop payments based on pre-determined criteria. • Ability to allow for audits and reviews. • Ability to prevent duplicate payments. • Incorporate warnings about the consequences of fraud in EDD documentation and forms. • Publicize successful DI fraud prosecutions on the EDD Web site and in the media to discourage fraud.	
3.4.3.1 (continued)	• Define and incorporate appropriate CalOHI practices and procedures. • Validate and ensure electronic acceptance, access, and storage for EIN. • Develop an automated interface with the EDD Tax System so employer names and addresses can be verified on-line. • Implement electronic acceptance, access, and storage for NPI.	www.ohi.ca.gov Employer Identification Number (EIN) assigned by the IRS National Provider Identifier (NPI) assigned by the National Provider System
3.4.3.2 Expand IT assets.	• Expand encryption to 100% for the new DI system. • Capability to define, use, and maintain electronic intelligent forms and applications. • Coordinate with PFL program to accept both PFL and SDI medical providers' information via direct electronic interface. • Capability to define, use, and maintain automated workflow. • Capability for complete testing, back-up, and recovery. • Provide training and technical knowledge transfer to EDD staff.	Compliance Reviews—160.308 Contingency Plan—164.308(a)(7)(i)

4.0 BASELINE ANALYSIS

The purpose of this section is to provide a clear understanding of the business and technical environment that currently supports DIB. The baseline analysis is comprised of the following sub-sections:

4.1   Current Method

4.2   HIPAA Analysis of the Current Method

4.3   Technical Environment

4.4   Existing Infrastructure

4.1 Current Method

The primary business functions performed by DIB include claim intake, monetary review, eligibility review, payment processing, overpayment review, Independent Medical Examiner (IME) review, document filing, appeals processing, and claimant service calls.

As depicted in Figure 4-1, Current DI System, the current DI application consists of both manual and automated components. Claim intake and document filing are completely manual in the DI environment; all other processes and sub-functions are primarily automated with some manual support, as indicated in the diagram process boxes. The primary automated system supporting the DI program is the DI system, which provides computer-assisted claims processing statewide. Additional automated processes include re-calculating claim amounts (re-computations), accounting processes (such as overpayment); and processing of benefit checks and forms.

Claim servicing is performed by a combination of staff and an Interactive Voice Response system (IVR). The IVR receives calls from a published toll free number. The caller is then given a choice of menu selections in the IVR for DI information. If the caller needs additional information, the caller can chose to speak to a DI representative. The calls are then distributed to staff through an Automated Call Distributor (ACD) system.

Figure 4-1. Current DI System
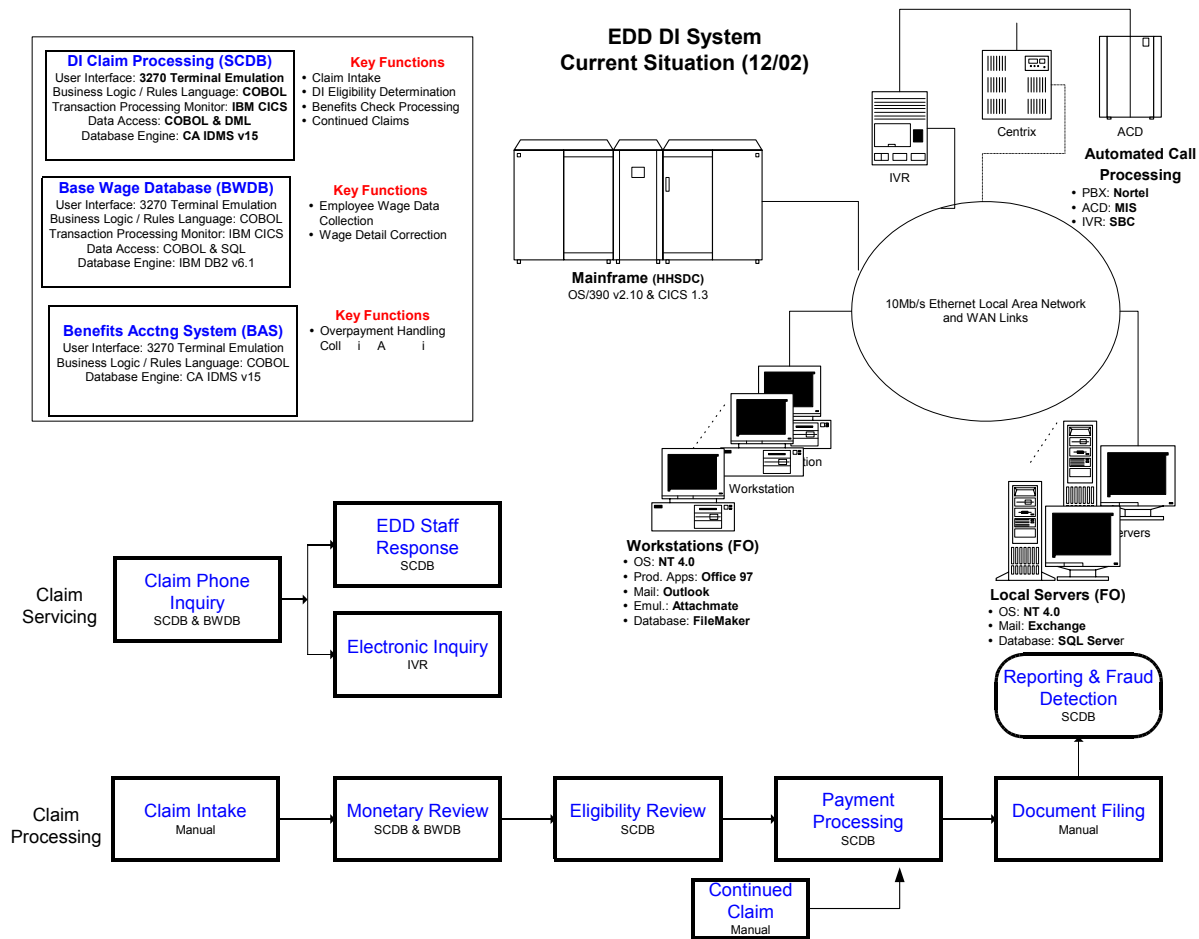
The SCDB is the central data repository for DI claimant-related data. The SCDB, originally developed in 1988, resides on an IBM S390 located at Health and Human Services Data Center (HHSDC). HHSDC provides hardware support for the system. SCDB runs on an Integrated Database Management System (IDMS) Database (a Computer Associates' product). It is the largest (IDMS) database of this type in the country. The SCDB is a two-tier mainframe-based solution, with PC-based terminal emulation ("green screen") access for EDD users. It is used to store and process approximately 750,000 DI claims yearly. It also stores and processes all UI claims. There are approximately 1,000 users of SCDB in DI, and closer to 6,000 users with UI, the Insurance and Accounting Division (IAD), and the Tax Branch. Client records on the SCDB contain claimant demographic information. Individual claim records contain information about a specific claim.

The DI program is also supported by the Tax Accounting System (TAS) which automates the monetary and non-monetary tax function (collection and tracking). Additionally, the DI program is supported by the Base Wage Data Base (BWDB), which stores employee's wage detail amounts reported by employers and the Benefits Accounting System (BAS) which processes overpayments and collection recompilations.

Currently, 52.4 IT PYs support the DI System. Figure 4-2 depicts the major functions and interaction of the DI system.

Figure 4-2. The EDD Single Client Database
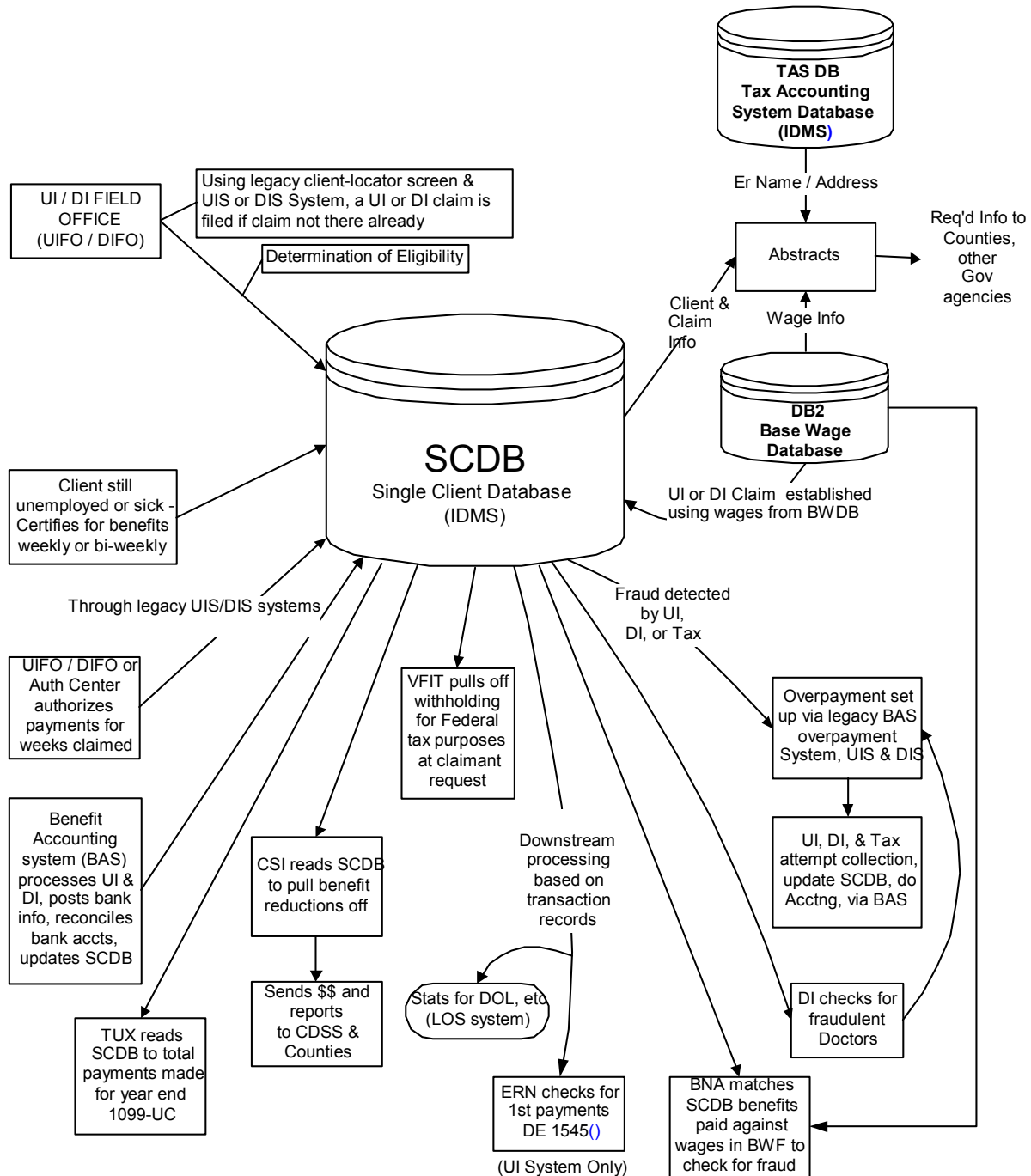
The DIB implemented the Family Temporary Disability Insurance Program, better known as the Paid Family Leave or PFL program in July 2004. The new automation put in place to support this program is a combination of existing EDD technologies modified to meet the PFL requirements and the development of unique PFL functionality on a modern technology platform. The new system consists of the following components:

- SCDB and DI application modifications

- PFL-specific functionality in a Web-based environment separate from the existing DI systems

- New Fresno facility programmatic support

- Integration of image scanning, OCR, and ICR technologies

- Integration of Call Center / IVR technologies

Information on the PFL system and its components can be found in the TEAM Feasibility Study Report, April 1, 1997, and Family Temporary Disability Insurance (FTDI) Feasibility Study Report, April 7, 2003.

4.1.1 Objectives of the Current System

The main objectives of the existing system are as follows:

- Provide timely and accurate DI payments to qualified claimants

- Track claims and claimant information

- Track medical provider information

- Track accounting and general ledger information

- Process appeals

- Combat abuse/fraud

- Provide services to claimants

The current automated system does not track claimant medical information beyond the initial claim codes. Any other medical information is collected and tracked via the manual paper-based system.

The EDD collects and analyzes data to support cases for prosecution and administrative action against those suspected of committing fraudulent acts. Within DIB are a Program Integrity Manager and 10 Field Office Integrity Specialists (FOIS) located throughout the State. The manager and the FOIS oversee, coordinate, and conduct various staff education efforts and investigative activities in the DI offices. The DIB staff work closely with EDD's Investigation Division's (ID) criminal investigators to combat fraud in the DI program.

4.1.2 Ability to Meet Current and Projected Workload

The DI business processes are constrained by the lack of flexible IT components. For example, DIB has 17 field offices that perform claims processing, but has difficulties allocating work processing across the workforce. If an office receives more claims than its local workforce can handle, workers must package and mail claimant paper case files to offices that have the capacity to take on additional workload. This attempt at balancing workload creates higher operational costs in the form of employee time to package, mail, and unpack paper case files. It decreases morale, delays processing of claims and issuing of payments, and inhibits responses to customer service calls.

Adding to the complexity of this problem, urban DI offices in high-density areas receive a higher number of claims than offices in less populated areas, and thus require a larger workforce to meet the workload. The cost of living in these urban areas is higher than in low-density areas, so recruiting and maintaining the workforce can be problematic.

The DIB's ability to process continual increasing workload in a timely manner is heavily dependant upon the current DI system, SCDB, TAS, BAS, and BWDB systems. Because these systems are built with outdated technology and the IT Branch has limited skilled resources, modifying these systems is arduous and costly.

The DIB's external stakeholders exchange information electronically in a HIPAA-compliant format. The DIB has not been able to keep pace with these agile business partners, especially its medical providers who are covered entities under HIPAA regulations. Most of DIB's medical provider business partners have complied with HIPAA by moving their data into electronic formats where they can provide better security and electronically transmit it. The DIB's medical provider business partners are very concerned about information security and privacy, and the timeliness and ease of information sharing.

As noted earlier in this report, DIB's current paper-based medical provider data exchange is mostly a manual process that is a time-consuming, laborious task for both DIB and its medical partners. One of HIPAA's primary directives is to compel the nation's medical providers and health care organizations to adopt a uniform claims standard, which favors electronic transmission of data and streamlines the information flow process and eliminates unnecessary time and labor.

The DIB's current IT systems do not support secure electronic transmission and reception of health-related data. The DIB is unable to interact electronically with claimants, medical providers, and employers. As a result, it is not in a position to benefit from the increased efficiencies afforded through electronic communication of data. The DIB cannot support its business partners' HIPAA and legislative mandates, nor meet its own automation goals.

4.1.3 Level of Satisfaction

4.1.3.1 Internal User Satisfaction

The DI system uses a mainframe-based user interface via terminal emulation ("green screen") rather than user-friendly graphical user interface (GUI). The current screens contain a great deal of information, are difficult to navigate, and users complain that the screens feel "cramped."

Additionally, the structure of the system often requires that users re-key information contained on one screen into another section of the database using another data entry screen. Existing screens do not have sufficient space to add additional data elements. Due to the older technology and lack of modern development tools associated with SCDB, it is a challenge to make changes to the system. Adding HIPAA specific functionality to the DI system would be difficult to do in a timely and cost-effective manner and would require a restructuring of the entire SCDB, not just the DI specific portions.

4.1.3.2 External User Satisfaction

External stakeholders interact with DI to share information. Information from SCDB is provided in paper-based hardcopy output to a number of stakeholders, including medical providers, employers, and the claimants themselves. Furthermore, DI exchanges information with other government agencies to validate claim and claimant data, investigate eligibility of claimants, cross-check information to uncover fraud or examine the duration of other State benefit programs, provide information for the adjudication of appeals, reveal child support obligations, and to file liens against Workers' Compensation Appeals Board cases. Information exchange is achieved primarily through file transfer protocol, email, mail, and telephone.

The DIB's largest medical provider, Kaiser Permanente has noted that they find the current paper-based interface to DIB's systems burdensome and inefficient. It requires them to download information from their automated systems and hand-write it into paper-based forms. In some cases, they then have to go back to their own automated systems to note the fact that they filled out a paper-based form. Kaiser's management has stated that they would find it beneficial if DIB were to institute more electronic processes and interfaces. Employers also interact with paper-based notification forms and if they want the information in their own systems, they have to key it in. Thus, the implementation of a more efficient system based on electronic transfer of data would benefit both the medical provider and employer stakeholder communities.

4.1.3.3 Technical Satisfaction

The SCDB and the subsidiary systems operate on IDMS database platforms. System developers use IDMS-DC and COBOL. Applications using the SCDB are written in COBOL, CICS, and IDMS DML. These platforms make support of the system very complex, requiring a significant amount of time and resources. Additionally, much of the original application development on the SCDB was accomplished using unstructured programming techniques. The unstructured and frequently modified application code and cumbersome mainframe tools make system changes difficult and costly, rendering the system inflexible.

Modifying unstructured code to implement complex business rules presents a continual challenge to programmers. DI Program changes already require frequent modifications to the DI system, straining existing technical resources. The technology platform makes migration to new technologies—even changes in printers—cumbersome.

IDMS is a non-relational database, a software technology that is over 30 years old. Modifications to the SCDB have resulted in the creation of thousands of test and training modular routines that have been developed over the years. The restructuring and testing of all the individual test and training modular routines that have been created and are now part of complex and interlocking machine code instructions causes extended delays and makes the

changes to the SCDB extremely difficult. Any new DI system must address system testing and user training and not rely on making copies of the production database to address these two business needs.

4.1.4 Data Input and Output

Table 4-1 summarizes the existing inputs and outputs of SCDB for the DI program.

Table 4-1. The DIB Data Input and Output

Inputs	Process	Outputs
U.S. Mail		Reports
Fax		Payments (checks) data
Walk-up	Manual Data Entry (SCDB)	Forms data
Phone & IVR		Automated Interfaces
Automated Interfaces		

Claimants currently submit DI information by fax, walk-up, and mail. The data collected is entered into SCDB via manual key data entry processes. In addition, for each claim, PHI is requested from medical providers using paper-based medical information forms, which are collected and stored at one of DIB's 17 field offices or two customer service centers.

As a service to claimants, EDD utilizes Automated Call Processing (ACP) and IVR to allow DI claimants access to pre-identified benefit information without requiring EDD staff intervention. The system includes PIN security authentication through SecureWay LDAP Directory services. The IVR/PIN system has specific safeguards added to protect claimant privacy and prevent unauthorized access to confidential information. The DI IVR/PIN system receives over 5 million telephone inquiries annually.

The DI system produces reports to employers, stakeholders, claimants, and doctors, and payments to claimants. Various reports are also generated for other entities. These are generated in a combination of hardcopy and electronic media.

Figure 4-2 outlines the data flows in and out of DIB and its ongoing business partners in administrating the DI programs. The majority of information flows in and out of DIB program via manual paper-based methods. The few fully automated electronic processes are shown in green and *italic bold* font, while the manual-based processes are shown in normal font. It should be noted that the graphic is a high level illustration meant to convey the fact that the overwhelming percentage of DIB's work processes are manually based. The graphic is an overview and the level of detail does not represent all of DI's complex work processes.

Figure 4-2. DI Branch Context Diagram
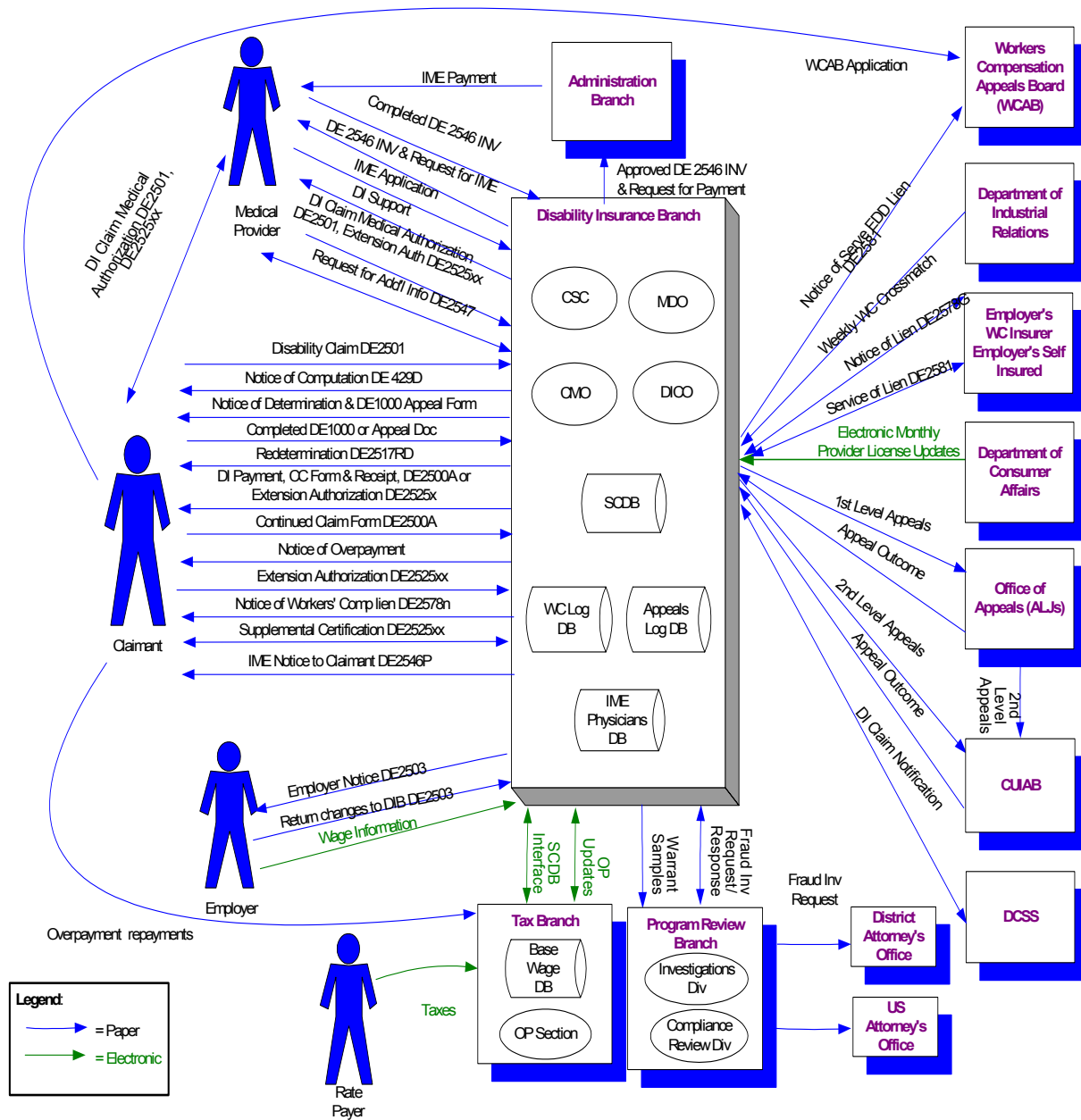
4.1.4.1 DI Process Overview

The following diagrams illustrate the interactions between internal and external entities involved in DI claims:

- Initial Claim (Figure 4-3)
- Continued Claims (Figure 4-4)
- Medical Extension (Figure 4-5)
- Employer Notice (Figure 4-6)
- Appeals (Figure 4-7)
- Workers' Compensation (Figure 4-8)
- Fraud Investigation (Figure 4-9)
- Overpayment Recovery (Figure 4-10)
- Data Sharing (Figure 4-11)
- Independent Medical Evaluation (Figure 4-12)

Diagrams are followed by descriptions of the functions.

Figure 4-3. Initial Claim
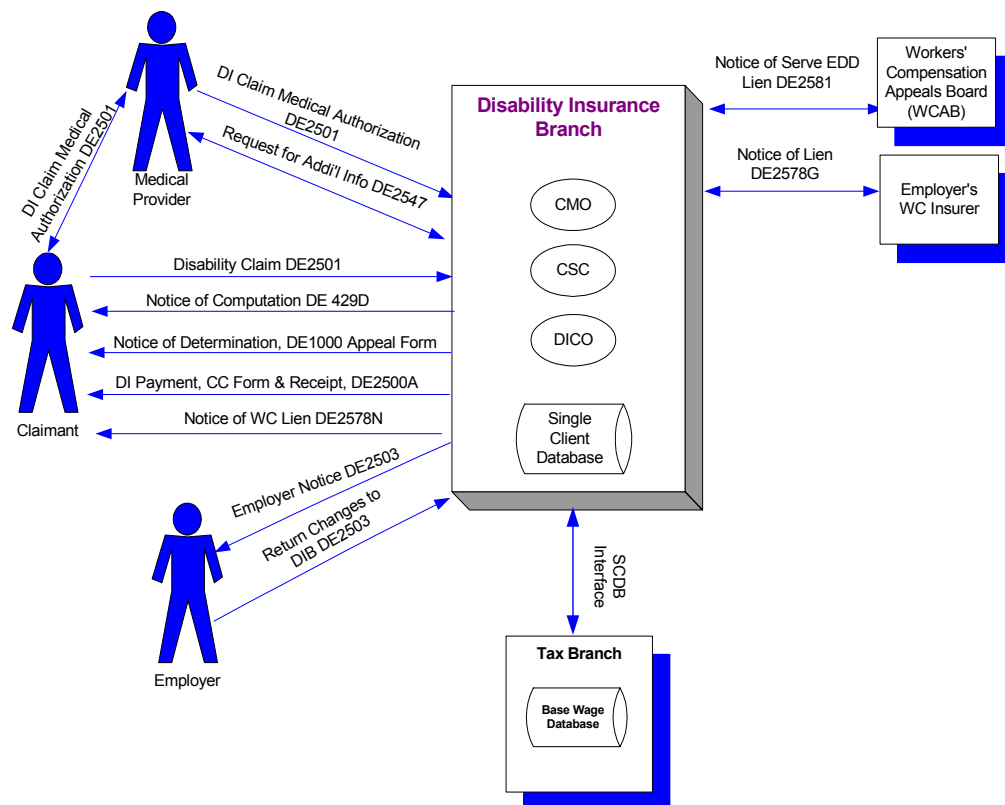
Initial Claim Process

These are the main steps in the processing of the initial (first) Disability Insurance claim associated with a particular illness or injury.

1. Prepare DE2501 Claim for Disability Insurance benefits (completed by claimant and medical provider).

   - Client/claimant completes their portion of DE2501 by typing or printing on the form, and then dating and signing it.

   - Medical provider (doctor) completes their portion and then dates and signs form.

   - Medical provider either submits DE2501 directly to DIFO or returns it to claimant for submission to DIFO. Submission may be made by mail, fax, or in-person delivery. Note: fraud potential is increased when the Client has access to the DE2501 (and therefore the opportunity to alter it) after the Medical Provider has signed it.

2. Receive, review, and sort claim forms (performed by Field Office clerical staff).

   - Separate DE2501s from other documents received and date stamp them.

   - Review for completeness and fraud indications.

   - If claimant's resident address and employer's mailing information is missing, attempt to obtain it by telephone.

   - Return applications lacking a signature.

   - Return any applications that are still incomplete.

   - Sort acceptable DE2501s, by SSN, into groups of up to 15.

3. Enter DE2501 data into the SCDB and verify provider information (performed by each Field Office key data operators).

   - Enter claim data into the SCDB via the State Plan Entry Screen

   - Verify medical provider address and license information against the Doctor Table and update if necessary.

4. Perform Monetary Review to determine if claim is monetarily valid (performed by Field Office Claims Examiner).

   - Review claims on SCDB (within Examiner's assigned SSN range) to verify that they are truly new claims. Any that are found to be continuations of prior claims are processed as described under Continued Claim Processing.

   - Verify that the SSN and claimant name are correct.

   - Check for prior DI and UI claims for patterns and impact on current eligibility for benefits.

   - Assign the EDD Claim Number (ECN) (if needed).

   - Determine the claim effective date (CED) and computation year.

   - Review base period wages using the Base Wage File to determine the existence and amount of eligible wages and the appropriate benefit award.

   - Review for potential fraud.

5. Perform Initial Claims Update (ICU) to determine the claim's eligibility (performed by CMO).

   - Determine the Unemployed Disabled Account (UDA) code by reviewing the claimant's prior employment/unemployment status for determination as to which account benefits are going to be paid.

- Review the claim for potential Workers' Compensation (WC) impacts. DI cannot be paid for the same period as WC unless the WC benefits rate is lower than the SDI benefit rate. Because DI is mandated to pay within 14 days, (claims that are otherwise determined eligible – CUIC 2701.5), but WC has up to 90 days to make a decision, claimants often file for both, and begin receiving DI benefits before a determination is made regarding WC. If the WC insurer denies the WC claim and the injured worker litigates the denial at the WCAB, then DI will file a lien against the WC insurer for reimbursement of DI benefits paid in lieu of WC. Note that Claims Examiners spend a significant amount of time resolving WC issues. See the Workers' Compensation section for additional information.

- Establish and enter disability commencement date (DCD).

- Verify that the claimant was in the labor market (either working or actively looking for work) at the time the disability occurred.

- Resolve issues by telephone or appropriate forms sent to claimants, employers, providers, etc.

- If the claimant is ultimately determined to be ineligible, or benefits must be reduced, or a portion of the claim is disallowed, such information is entered into SCDB and a Notice of Determination (DE2517) is issued. See Adjusting or Disqualifying Claims in the HIPAA Transaction and Code Set Gap Analysis Report for additional information.

- If any wages used in the initial calculation should not have been used, make a request for re-computation, and Issue a Notice of Determination (DE2517) for any CED adjustment made affecting the base period.

- Document actions and any potential issues in the "claim notes" in SCDB.

6. Review medical information and implement Duration Control if needed (performed by CMO).

- Review the medical information originally provided on the DE2501 that is now in the SCDB (note that not all information provided on the DE2501 is entered into the SCDB – Claims Examiners sometimes have to go back to the hardcopy for detail).

- The DIS/SCDB calculates the normal expected duration of the disability (and corresponding benefit) based on the disability commenced date (DCD) and the International Classification of Diseases (ICD) diagnosis code of the illness or injury.

- If the expected duration that is stated on the DE2501 materially exceeds the normal expected duration of that illness or injury based on DIB's policies, duration control procedures may be performed (based on the discretion of the Examiner, specifics of the case - age, occupation, and medical condition; and published guidelines). Duration control actions may include: telephone inquiry to the medical provider or claimant, disability status questionnaire sent to claimant, request of the medical provider to provide additional medical information, or request for independent medical examination (IME).

- Document actions or potential issues in the "claim notes" in the DIS/SCDB.

7. Adjust or disqualify claim (performed by CMO).

- Review base period wages to verify existence and amount of eligible wages using the Base Wage File.

- A re-computations process (RECOMP) is implemented when there is a need for change on the claims record (e.g., if any wages used in the original calculation should not have been used, request that the DIS/SCDB recalculate the benefit award).

- Issue a Notice of Determination (DE2517) for any Claim Effective Date (CED) adjustment made affecting the base period.

- Eligible claims may be suspended while waiting for necessary information or while the Claims Examiner obtains documentation.

- Employer and medical certifications on existing claims are reviewed by Claims Examiners.

8. Authorize payment of benefit (performed by CMO).

- If all claim issues are resolved and the claimant is determined to be eligible, authorize payment of the benefit (the claim is "qualified for payment"). DI is required to make a decision within 14 days of claim receipt.

- Most claims require the claimant to submit biweekly certifications in order to continue receiving benefits.

- The DIS/SCDB system identifies claimants qualifying for continued claims payment. See Continued Claim Processing for additional information.

- Depending on the claim duration (whether it is six weeks or longer), the claim will go into automatic payment mode (ATP). There will be no required continued claim forms sent out to the claimant until the last week of the ATP period. At ten weeks from the date of the claim, form DE2593 is sent to the claimant requesting verification of whether the claimant is still disabled or has returned to work.

- Original (hardcopy) claim forms and related documents are filed in the Correspondence File by clerical staff in each field office.

Figure 4-4. Continued Claim
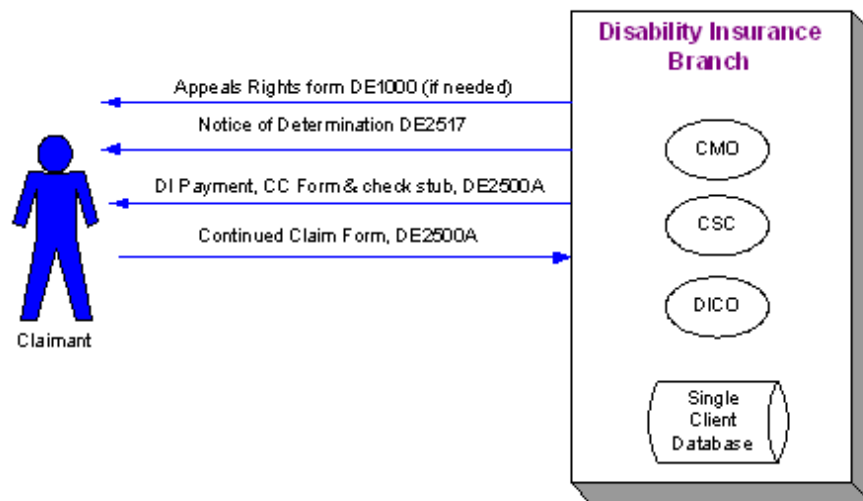
Continued Claim Process
Continued claims require the claimant to send a DE2500A to the CMO every 2 weeks to continue receiving benefits (within the expected duration period identified on the original claim). This is the most common type of DI claim.

1. Prepare DE2500A Claim for Continued Disability Benefits (performed by claimant).

- Client/claimant receives DE2500A (also called a "Continued Claim Certification") with their benefit check. This specifies a specific time period during which the claimant is requested to certify that he or she was disabled and unable to work, in order to continue receiving DI benefits for that period.

- The claimant is also required to list all monies received from any source during the specified time period. This includes wages, sick leave benefits, and Workers' Compensation benefits.

- Changes to address or telephone number should also be reported on the form.

- The claimant is required to sign and date the DE2500A to certify that all information on the form is true and correct.

- The claimant should return the DE2500A to the CMO *after* the date indicated on the form. If it is returned earlier than the specified date, DI benefits can only be paid up to the postmark date or the signature date, which ever is the earliest. Returning the form early results in shortening the benefit payment period.

2. Receive, review, and sort Continued Claim Forms (performed by CMO Clerical Staff).

- Separate DE2500A from other documents received and date stamp them.

- Review for completeness and fraud indications.

- If information is missing, attempt to obtain it by telephone.

- Return forms lacking a signature.

- Sort DE2500As into: (1) claims that go to key data entry for batch payment, (2) no key data entry, and (3) continued claims that need to go to a Claims Examiner for review.

3. Enter DE2500As not requiring Claims Examiner review into DIS/SCDB (performed by CMO key data operators).

- Enter continued claim data into SDCB via the batch payment screen.

- This triggers a continuation of benefit payments.

4. Review remaining Continued Claims (performed by CMO).

- Process continued claim requests requiring Claims Examiner review in much the same way as original (new) claims, including review of eligibility, payment, and medical information. See Original Claim Processing, steps 4-6 for details.

- Implement duration control procedures if necessary (e.g., request and IME, send out medical request forms or contact either the doctor or the claimant with questions).

5. Authorize or deny continuation of benefit payments (performed by Field Office Claims Examiner).

- If all issues are resolved and the claimant is determined to be eligible, the continued claim is processed in DIS/SCDB so that benefit payments continue.

- If the request is determined to be ineligible, it is disqualified, and a form is sent to the claimant. If fraud is suspected, benefits may continue while the investigation is under way.

- Original (hardcopy) DE2500A forms and related documents are filed in the Correspondence File by clerical staff.

Figure 4-5. Medical Extension
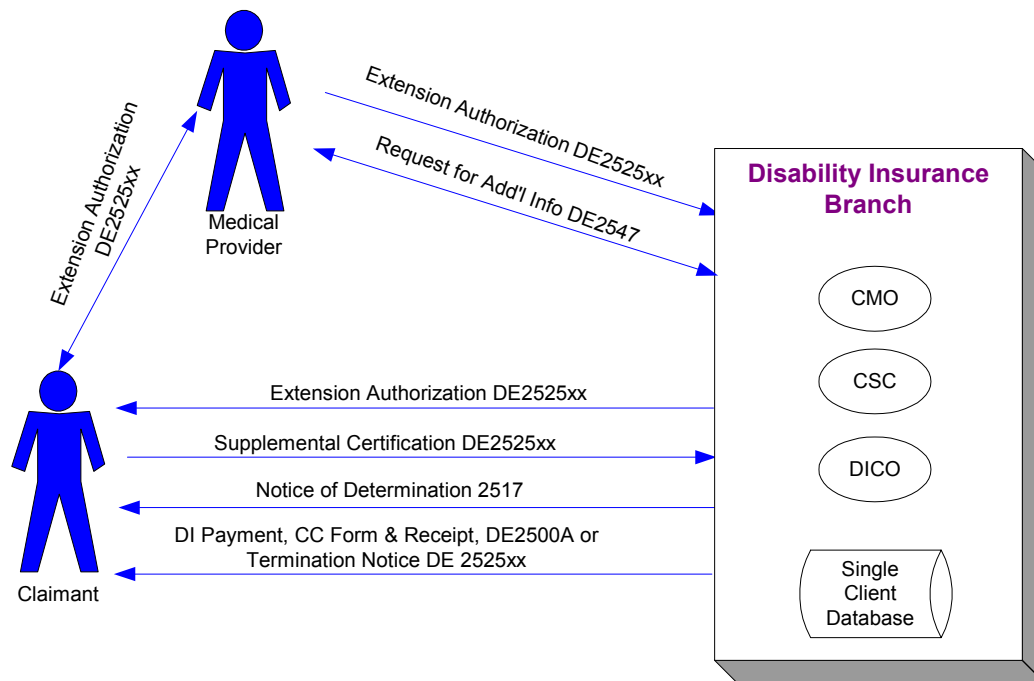
Medical Extension Process

This applies in situations in which a claimant remains disabled by illness or injury (and is therefore unable to work) beyond the expected duration specified by the Physician in the initial DE2501.

1. Prepare DE2525xx Physician's Supplemental Certificate (performed by claimant and medical provider).

    • Client/claimant receives DE2525xx with the notice final payment of benefits. A medical provider determines the return to work date. They will state when the claimant is able to return to their regular or customary. This is the new prognosis date.

    • Client/claimant takes DE2525xx to his or her medical provider.

    • Medical provider (physician) completes, signs, and submits the DE2525xx to the DIFO or gives it to the claimant. Submission may be made by mail or fax or in person.

2. Receive, review, and sort (performed by clerical staff).

    • Clerical staff separate DE2525xxs from other documents received and date stamps them.

    • Review for completeness and fraud indications.

    • If information is missing, attempt to obtain it by telephone.

    • Return certifications lacking a medical provider's signature.

3. Review Doctor's Certification (performed by CMO).

    - Review the Doctor's Certification that extends the expected duration of an existing claim and medical disability advisor's (MDA) documentation. (Compare with original data in SCDB, as well as any additional data on the original DE2501.)

4. Authorize or deny Extension of Benefit Payments (performed by CMO).

    - If all issues are resolved and the claimant is determined to be eligible, the extension is processed in DIS/SCDB so that benefit payments continue.

    - If the request is determined to be ineligible, it is disqualified, and a Notice of Determination is sent to the claimant. If fraud is suspected, benefits may continue while the investigation is under way.

    - Implement duration control procedures if necessary (e.g., request an IME, send out medical request forms or contact either the doctor or the claimant with questions).

    - Original (hardcopy) claim forms and related documents are filed in the correspondence file by clerical staff.

Figure 4-6. Employer Notice
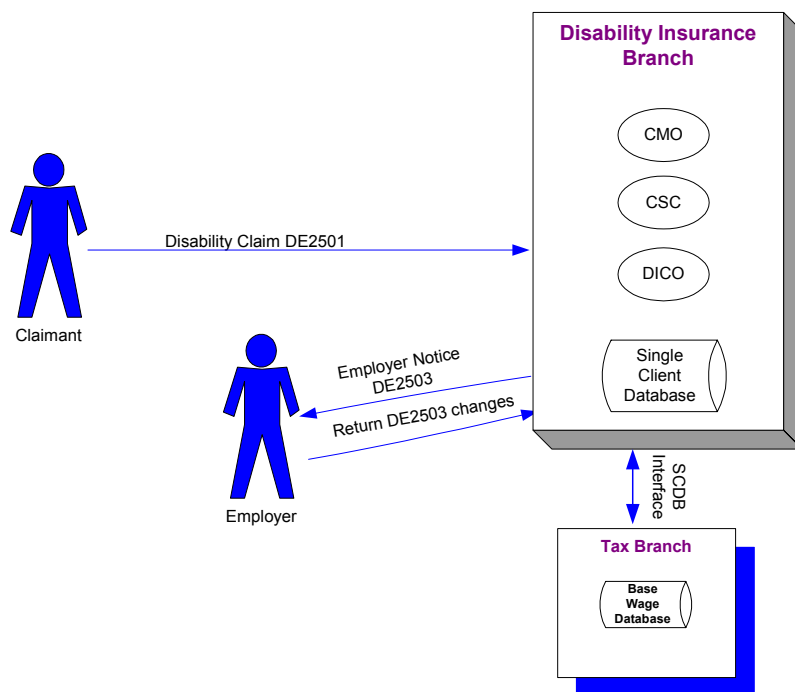
Employer Notice Process

For each new claim submitted, DIB attempts to validate the employee's status with their stated employer.

1. Entry of the original claim (DE2501), as described in Original Claim Processing, Step #3, triggers the mailing of an Employer Notice (DE2503) to the claimant's employer requesting confirmation of claimant eligibility information, past or current employment and if they are entitled to any pay.

2. Employers must notify DIB within 2 days only if they have information that differs from that provided by the claimant. The DE2503 states that an employer is required to mail back the form if there is any information different than what is stated about their employee. If there is no change the form does not need to be returned.

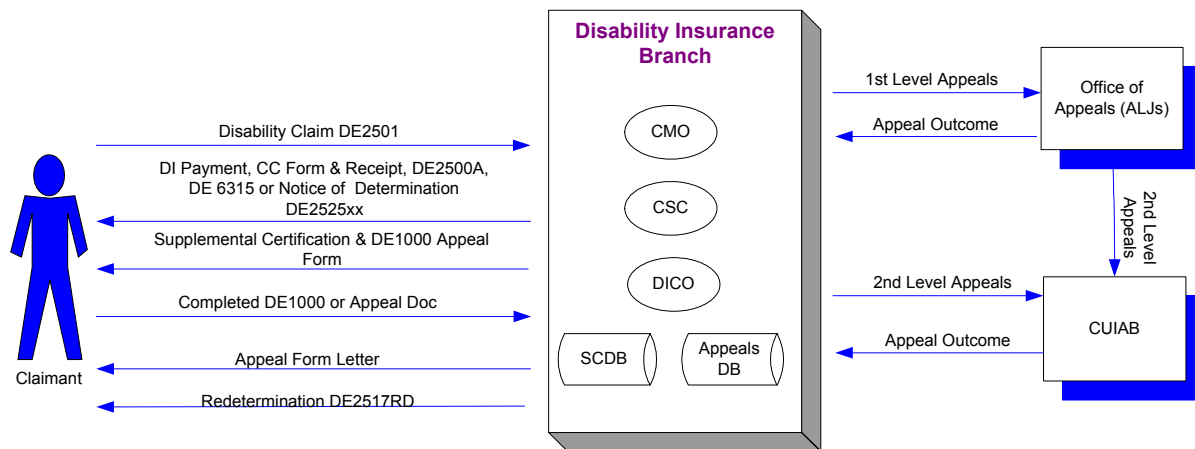3. The Claims Examiner takes any action required to confirm or correct employment information, and makes any required adjustments to benefit payments that result, and issues a Notice of Determination (DE2517) if necessary.

4. Everything is documented in notes on the DIS/SCDB, and the hardcopy DE2503 is filed.

Figure 4-7. Appeals

Appeals Process

A claimant is entitled to appeal a negative decision made by the DIB in regard to their disability claim.

1. A Notice of Determination is sent to the claimant for notification of any level of denial. This is a form with a large number of selectable reason statements and the ability to author a custom statement. Along with the Notice is sent a DE1000 that contains instructions on how to file an appeal and can be used as the appeal document.

2. If the claimant appeals the disqualification, an Appeals Specialist reviews the claim.

3. Claims can be re-determined to be eligible by a Claims Examiner if the claimant supplies the necessary information.

4. The Appeals Specialist has the option of re-determining an appealed claim based on new information or the discovery of an error in the initial processing.

5. Appealed claims that are not re-determined to be eligible may move on to a hearing before an Office of Appeals Administrative Law Judge. This hearing is attended by the Appeals Specialist. Benefits may be paid during the appeal process if the claimant requests them pending the appeal decision and is otherwise eligible. A DE6315D is sent to the claimant for this purpose. The DE2500A and DE2525XX may also be sent to claimant to be signed and returned.

6. If the appeals decision is contrary to either the claimant or DIB and this does not produce the outcome desired by the claimant or DIB, that party may appeal to the California Unemployment Insurance Appeals Board (CUIAB) as the 2nd Level Appeal.

Figure 4-8. Workers' Compensation
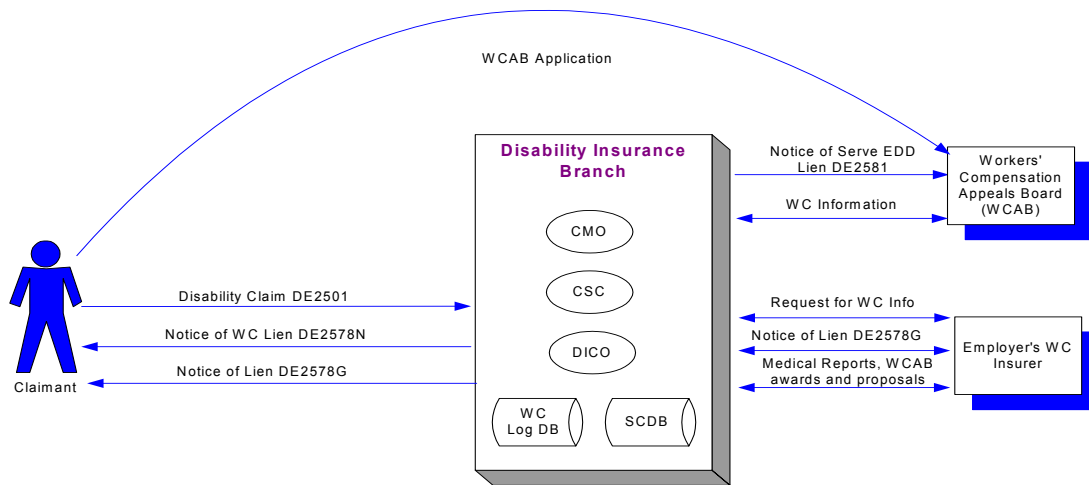
Workers' Compensation Process

The DIB attempts to contact the employer's Workers' Compensation insurer when claims are submitted which indicate a work-related illness or injury.

1. In the case of initial claim, the Claims Examiner reviews the claim for indications that disability was caused by employment. Determination of Workers' Compensation insurers acceptance of liability is then performed.

2. If the WC benefit rate is less than the SDI benefit rate, then the claimant is eligible for DIB benefits that make up the difference between the two rates.

3. WC carriers or self-insured employers may voluntarily reimburse DI for duplicate payments that were made.

4. When a potential industrial injury or illness is indicated and the insurer or self-insured employer has not accepted liability, the Claims Examiner will qualify the claim for payment if otherwise eligible. The WC insurer has up to 90 days to accept or deny; however, DI must pay within 14 days. In these cases, a notice of lien claim (DE2578G) is filed against the WC insurer for future reimbursement of payments and notice DE2578N is sent to the claimant.

5. When WC liability is denied by the WC insurer and the claimant disagrees and files with the WCAB, and DI files a lien on the case, all further actions are handled by the WC Specialist.

6. The WC Specialist represents DI at all WCAB proceedings and resolves the DI lien as part of the WCAB case resolution.

7. WC claims with overpayments are referred to overpayment specialists for recovery of funds.

Figure 4-9. Fraud Investigation
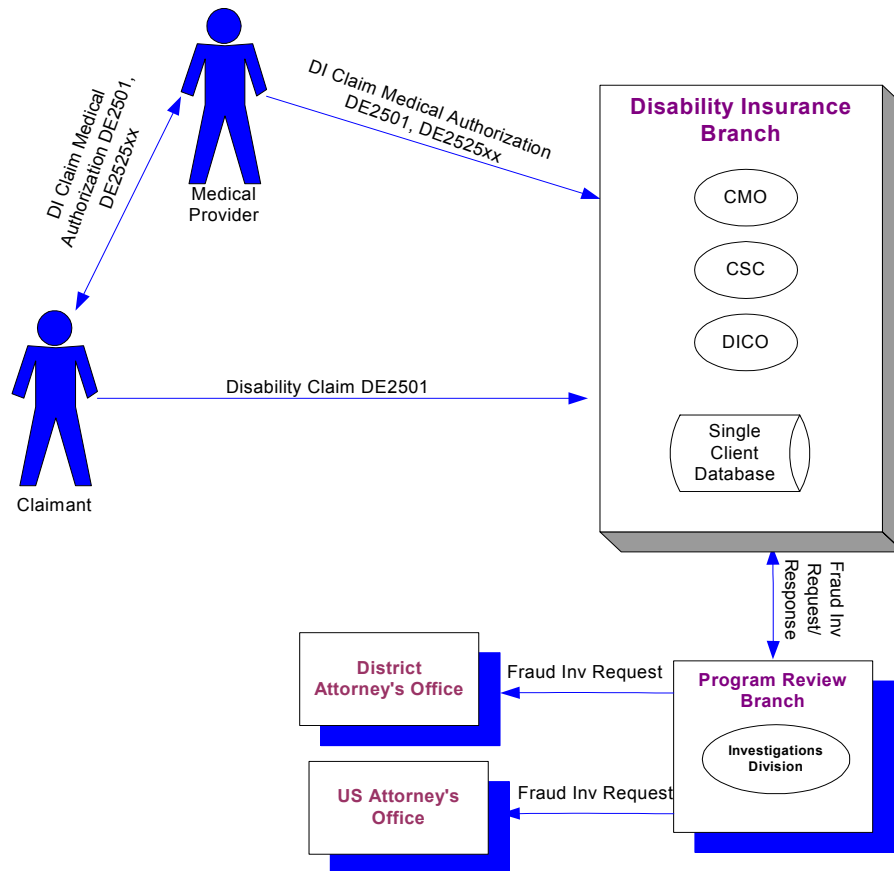
Fraud Identification and Investigation Process

Many steps in normal claim processing include elements of fraud and abuse detection and prevention (for example: reviewing documents, verifying information, implementing duration of payments control, etc.). However, this section will focus on the more fraud-specific processes.

1. Reports are made available to the DI program integrity staff, who review them to detect potential fraud and abuse. Flags are placed on claims to prompt DI staff to investigate further.

2. The DI system prompts the Claims Examiner to check the Program Integrity Bulletin Board on the DI server for any special handling instructions relating to potentially abusive or fraudulent claim activities on claims certified by specific doctors.

3. DI program integrity staff enter information into the Microsoft Excel-based "Desk Top Database" and "Doctor Tracking System."

4. DI program integrity staff review the flagged claims looking for additional indications of fraud.

5. In addition to this proactive identification of potential fraud occurrences by the DI program integrity staff, they also receive referrals from Claim Examiners who may identify potential cases of fraud in the course of reviewing claims.

6. An additional source of potential fraud is the Fraud Reporting Hotline operated by the EDD ID's Criminal Intelligence Unit (CIU).

7. When evidence reveals a pattern of fraud, the ID initiates a case in the claims management information system (CMIS). The Case Face Sheet is printed and placed in the case file, and the case is assigned to an Investigator.

8. The Investigator, sometimes with assistance from the DI program integrity staff, gathers documentation and researches the case, looking for patterns, discrepancies, etc.

9. If multiple claims or cases appear to be linked, information about them is compiled into a "Desktop Database" to facilitate managing the details of the case.

10. The purpose of the investigation is to identify and prosecute suspects who perpetrate fraud schemes against the DI program.

11. During the course of the investigation, the investigator will obtain a variety of documents and evidence necessary to support a criminal filing.

12. The Investigator may request assistance from external criminal justice entities to process subpoenas, compel testimony, obtain search warrants, etc.

13. When the investigation is completed, if there is sufficient evidence, the case is referred for prosecution.

Figure 4-10. Overpayment Recovery
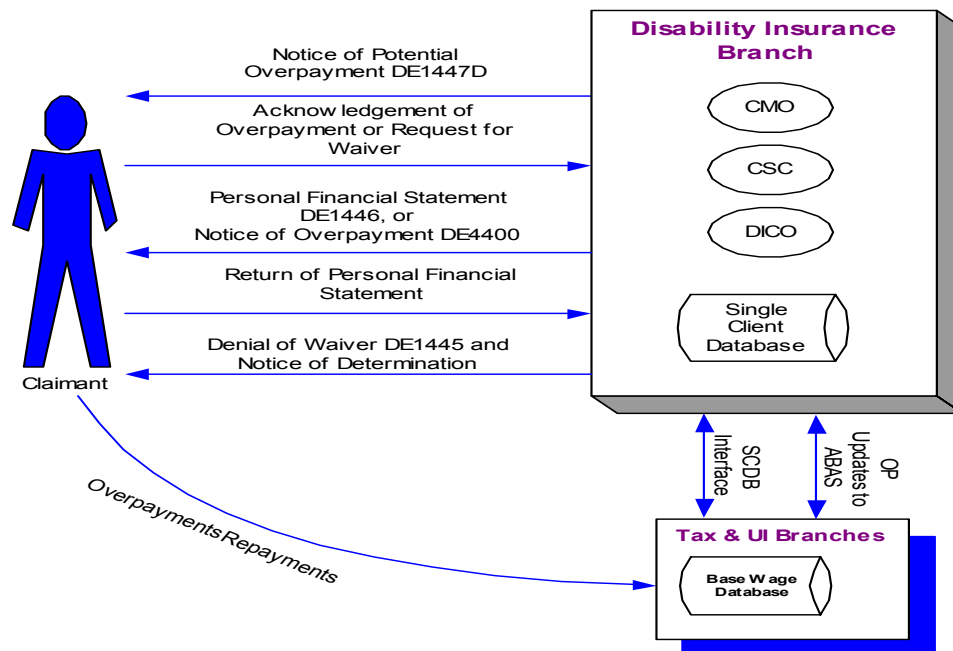
Overpayment Recovery Process

Overpayments can result from several different situations. Examples include the employee's benefit amount being incorrectly computed for reasons of inaccurate base wage information, or the employee returns to work and DIB is not notified. In situations such as these, DIB takes action to recover the overpayments from the claimant.

1. Notice of potential overpayment and waiver overpayment documents DE1447D are sent to claimant.

2. Overpayment Notice DE4400 sent to claimant

    - Claimant has 20 days to appeal overpayment notice.

    - Claimant can request consideration of waiver and documents to waive overpayment.

3. Personal Financial Statement DE1446 sent to claimant if they request waiver.

4. If no waiver requested, claimant is directed to contact the claims examiner at the CMO.

    - Payment schedule can be arranged.

    - Payments are made to EDD.

5. After review of claimants Personal Financial Statement, DIB will send either Denial of Waiver DE1445 or Notice of Determination.

6. If Denial of Waiver, after 30 days, case is referred to Tax Branch for collection.

    - Case is handled by Benefit Overpayment Collection Section (BOCS).

    - BOCS then updates the SCDB with payment information.

Figure 4-11. Data Sharing
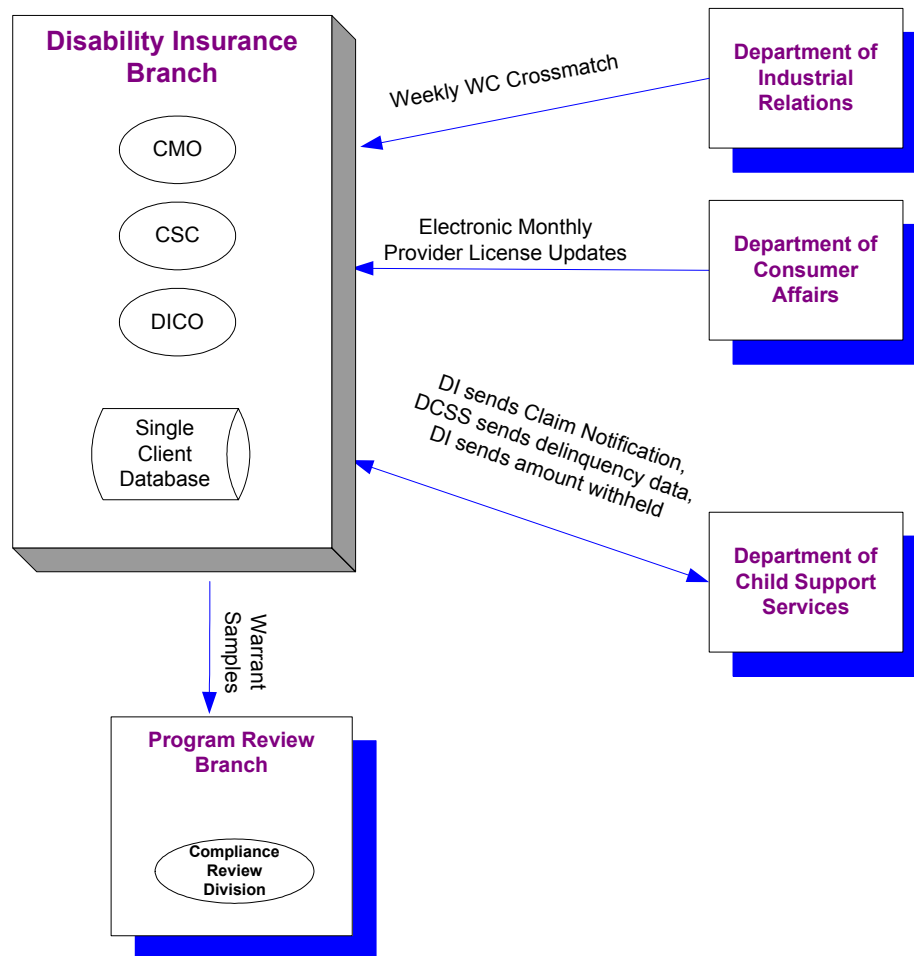
Data Sharing Process
DIB interfaces with several external entities to share data for various purposes.

1. Department of Industrial Relations – Provides DIB with weekly workers' compensation cross match report of claimants who filed a case with the WCAB and the SSN matches a SDI claim.

2. Department of Consumer Affairs – Provides DIB with a monthly electronic medical provider license information updates.

3. Department of Child Support Services - DI claim information is transmitted to this department and compared to their database so that DI payments can be garnished if the claimant is in default on child support payments.

4. Compliance Review Division – The EDD Quality Control Unit (QCDI) randomly selects warrants for audit purposes and reviews the associated claim information cases to ensure compliance with EDD and DIB policies and procedures.

Figure 4-12. Independent Medical Evaluation
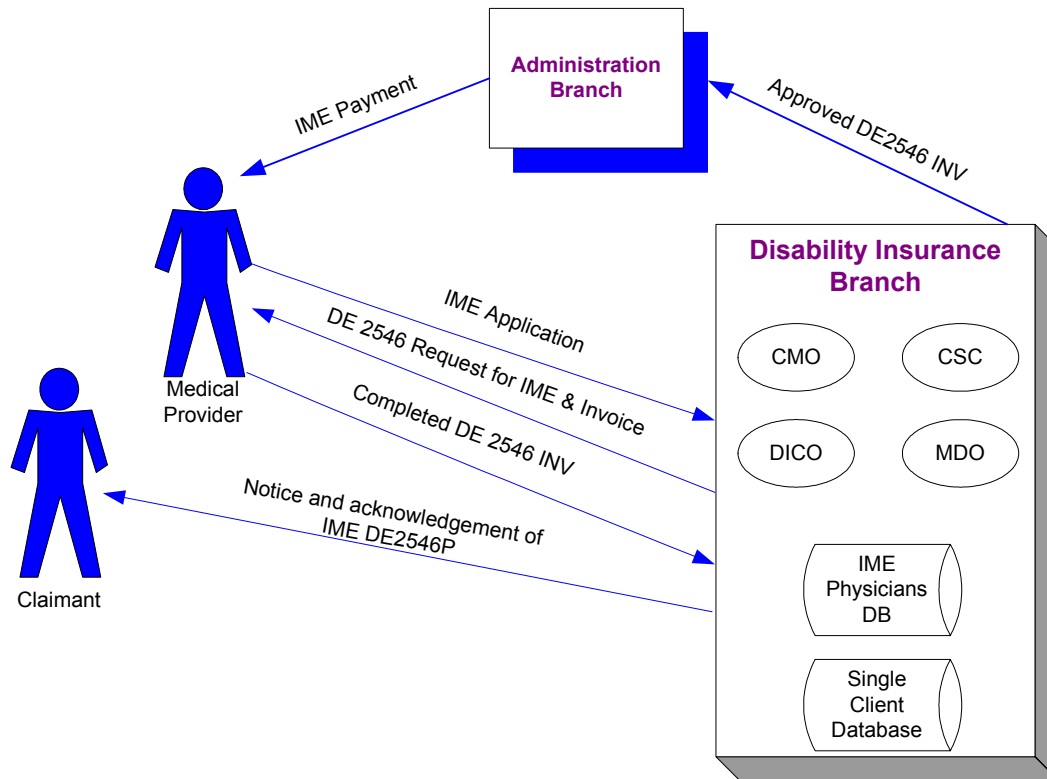
Independent Medical Evaluation (IME) Process

The Medical Director's Office evaluates and approves medical providers to conduct independent evaluations of claimants at DIB's request. These medical providers apply to EDD and go through a certification process prior to being accepted into the program. After certification, claims examiners will send paper requests to claimants identified for IMEs.

1.   The DIB sends the IME form DE2546 along with a request to perform the IME.

2.   The DIB sends form DE2546P to the claimant to request that he/she schedule the IME appointment and notify the DI program of the date and time.

3.   The IME doctor performs the evaluation and returns the DE2546INV to DIB with the results of the exam.

4.   The DIB reviews the exam results and takes the appropriate action. The medical report information is entered into notes fields on the SCDB and then is filed.

5.   The DIB reviews the invoice, makes any necessary corrections, and forwards to EDD Fiscal for payment to the IME doctor.

4.1.5 Data Characteristics

SCDB contains approximately 1.4 billion records. It is used to process more than 3 million online transactions per day using CICS screens and VSAM files. Upon completion of online transactions, batch processes are used to accomplish tasks such as check processing for UI

and DI. Client records contain claimant demographic information such as name and address. Individual claim records contain information about a specific claim, such as: claim effective date, amount of benefits, and checks issued.

Because of the current system's low level of inherent business logic, operator cues, and data element filters, the current manual data entry process affects DIB's ability to obtain a higher level of data integrity which is generally provided by more modern systems.

4.1.6 Security, Privacy, and Confidentiality

The EDD Information Security Office has the primary responsibility for setting policies and procedures for security within EDD. To ensure the highest security, EDD employs security provisions at the network, application, and data levels. The current technology environment addresses security on each of its platforms including using IBM's Resource Access Control Facility (RACF) on the mainframe and Windows security on the desktop.

At the network level, the HHSDC firewall and security mechanisms within routers at both HHSDC and EDD provide restricted access. Access into the department's network is password-protected. Unsuccessful attempts to logon to a system result in a User ID being disabled. Remote users, with proper security, have access to SCDB through the HHSDC firewall.

At the application level, EDD employs user authentication and authorization routines to limit access based on internal policies. There are different roles based on access levels within the applications (e.g., update and inquiry) and segregated access to screens within the applications.

At the data level, EDD makes every effort to ensure the integrity of its data while limiting fraudulent information and maintaining the privacy and confidentiality of stakeholders who interact with the DI program. Security issues at the data level include:

- **Data integrity.** It is important that the public has trust in the integrity of the DI program; thus DIB takes great efforts to ensure that its data is accurate and reliable.

- **Fraud**. Likewise, fraud detection and prevention are important to the DI program. As described in a 2001 KPMG report, the industry fraud rate is estimated at 1.5%.

- **Privacy. The DIB** receives and retains data that must be protected by HIPAA covered entities in accordance with federal law and regulations. While EDD is not technically a HIPAA-covered entity, claimants, medical providers, and state policy makers have a reasonable expectation that EDD will also take comparable measures to protect the privacy and confidentiality of claimant PHI.

4.1.7 Equipment Requirements

The SCDB system resides on a Health and Human Services Data Center (HHSDC) mainframe. All DI employees access the SCDB through their PCs using TN 3270 terminal emulation. In the call centers, the SCDB system interfaces indirectly with SBCM Periphonics Call Center systems (ACP and IVR) to access a VSAM file, which contains extracted payment data from the SCDB.

DI has a single, common PC platform for desktop computing, e-mail, and HHSDC access. All of the PCs are networked to the central office; network equipment is primarily standardized on Cisco products.

4.1.8 Software Characteristics

Software characteristics include examination of application development tools, operating system software, personal productivity software, and enterprise communication software used by SCDB:

- **Application development tools**. The SCDB application is built in the IDMS relational DBMS from Computer Associates. It runs on a mainframe platform and incorporates COBOL as the high level programming language. The standard application development tool set is EDD's mainframe Programmer Workbench and Change Man. Other application development tools include EasyTrieve, SyncSort, Xpediter, FileAid, AbendAid, and DYL280.

- **Operating system software**. The SCDB mainframe operating system (OS) is OS390 (v2.10). At the desktop, PCs run on Microsoft NT 4.0.

- **Database software**. SCDB utilizes IDMS (v15). The size of the database is documented in Section 4.1.7.

- **Personal productivity software**. Microsoft Office 97 Professional is the standard personal productivity software within EDD. The Microsoft Office suite includes Word, Excel, PowerPoint, and Access. In addition, FileMaker Pro databases, Symantec PCAnywhere and Attachmate Extra (for 3270 terminal emulation) are in use.

- **Enterprise communication software**. The EDD staff utilizes Microsoft Outlook for all enterprise e-mail communication.

4.1.9 Internal and External Interfaces

The DIB's current processes encompass multiple internal and external interfaces. Internal stakeholders have access to the SCDB system to conduct claim submission, monetary and eligibility review, and disbursement and accounting functions. Other internal stakeholders are recipients of the system outputs, such as management and operational reports. DI interfaces with other State agencies to exchange information to limit the incidence of fraud, validate eligibility and claims information, and to provide output from the DI system.

It should also be noted that even in situations where internal and external electronic interfaces exist, numerous problems still must be overcome. Although the data can be sent electronically to internal and external business partners, the data is not necessarily presented in the same format as the receiving agency can utilize. Often there are application software version discrepancies, reformatting, or other data staging problems that must be overcome; and lastly, the information may not be presented in the manner the receiving entity requires or prefers.

Internal and external stakeholders with which DIB interacts are provided in Sections 3.1.1.2 and 3.1.1.3. Interfaces are achieved primarily through a combination of file transfer protocol (ftp) and diskette. System interfaces are documented in Table 4-2.

Table 4-2. Overview of Internal and External Interfaces

Internal	External
Unemployment Insurance – Both the UI and DI program use the SCDB. The UI program has access to DI data via automated business rules. Information Technology Branch – Read and update access on a very limited basis. Tax Branch – Access on as-needed basis. Office of Documents Publications and Distributions - Input and output only. Assists in development of Forms Note: DIB has similar unit. Insurance Accounting Division – Access and output. Program Review Branch, CRD – Access on as needed basis to conduct case reviews.	Department of Industrial Relations – Provides data (input), which is uploaded in batch mode. Department of Consumer Affairs – Provides data (input), which is uploaded in batch mode. Department of Child Support Services – Provide data (input) and receive benefits withheld from the non-custodial parents. Department of Health Services – Provides data (input), which is uploaded in batch mode.

4.1.10 Personnel Requirements

There are currently a total of 1,660.9 budgeted positions assigned to the DI program. Approximately 73 percent of this workforce is located in DIB's Field Offices and are dedicated primarily to providing services to claimants and the processing and management of claims. The size of this field force increases or decreases with the volume of claims and is determined by the minutes per unit (MPU) DI staff spend processing claim related documents. The workload balancing problem DIB faces as a result of this situation creates efficiency and cost problems. This workforce is supported by other personnel who work in the Central Office as well as a number of other EDD support units. Additionally, the SCDB system is supported by a total of 52.4 technical positions that are part of the IT Branch.

4.1.11 System Documentation

Documentation for the SCDB system exists; however, there are issues with its currency. New modifications to the system are not well documented. Given the frequency of modifications to the system, this is a significant problem that could have long-term repercussions in terms of supporting and troubleshooting the system. Documentation is in various media, hard copies, and soft copies.

4.1.12 Failures of the Current System

Although SCDB is not been prone to operational failures, there are risks to the system if SCDB is restructured to be the repository of all intended HIPAA administrative simplification transaction information. The major risk areas are:

- SCDB technical limitations increase the difficulty of adding additional data fields.

- While the DI system is capable of handling anticipated HIPAA administrative simplification transaction volumes, the ability of SCDB to accommodate numerous changes to its data structure is problematic.

EDD Employment
Development
Department
State of California

DI Automation Project, Phase 3
Feasibility Study Report

- The current system is a paper-driven system and relies on manually keyed data. Manual data entry increases the likelihood of errors, which can impact payments of benefits to qualified claimants.

- Currently PHI is requested by mail or fax and stored in unlocked files in one of DIB's 17 field offices or two customer service centers.

- The current system does not have the capability of accepting or recognizing electronic signatures.

4.2 HIPAA Analysis of the Current Method

The Protected Health Information (PHI) flow is shown in Figure 4-13. Accompanying this illustration is a description of the units in DIB and the business functions that are integrated with this information flow.

Figure 4-13. DI Branch PHI Flows
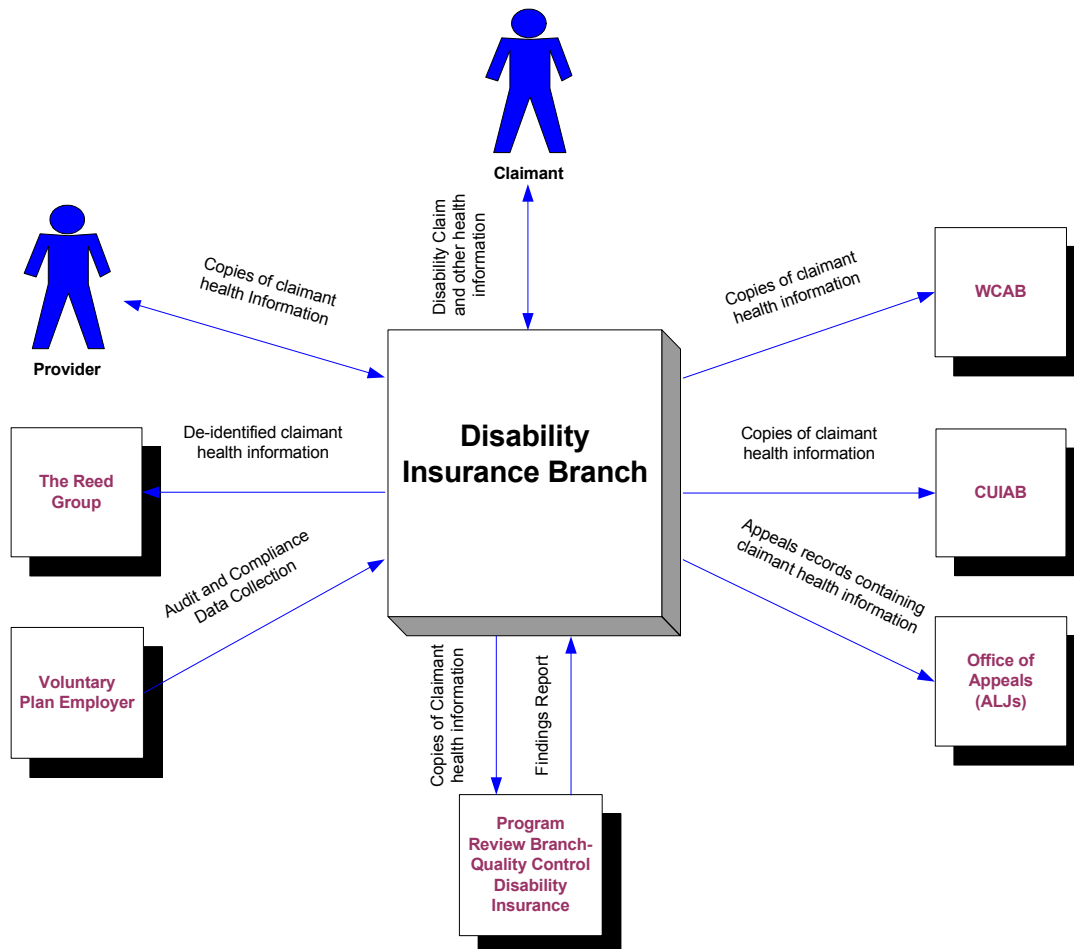
Medical Director's Office

The Medical Director's Office is responsible for approving physicians for the Independent Medical Examination panel, reviewing fitness for duty and reasonable accommodation files, and is a source to EDD offices with medical concerns.

The Medical Director's Office may receive calls from claims examiners regarding issues with claims and, as a result, view or receive health information, but this does not happen regularly. Other instances where the Medical Director's Office may receive health information occur when Medical Extensions or other forms are sent to this office accidentally. Those documents are either re-routed back to the claim holding office or shredded.

Health information received and stored by the Medical Director's Office includes fitness for duty and reasonable accommodation files that require review by the Medical Director. These files are stored in the Medical Director's Office in a locked filing cabinet. Only appropriate, Medical Director's Office personnel have access to these files.

Any marketing that is done by the Medical Director's Office is for public acknowledgment of EDD services only, not audience specific. Health information of claimants is not used to target groups for marketing.

Program Review Branch - Quality Control Disability Insurance Unit

The Quality Control Disability Insurance Unit (QCDI) is under the Program Review Branch and is responsible for reviewing claims in their entirety and issuing findings on discrepancies within the Disability Insurance Branch benefit payment systems. Health information is received from providers in order to verify medical information on the claim. Health information may also be received from the claimant during discussions of claim information.

The reviewed claims are pulled from a random sample of 20 to 25 checks that were issued the previous week. From those checks, the Social Security Numbers are used to request copies of claim documents from the field office. A questionnaire is sent to the last employer to verify the employment information. Another questionnaire is sent to the provider to verify the diagnosis, dates seen, and other medical information. The last questionnaire is sent to the claimant with a request for an appointment to discuss the claimant's information. After all of this information is collected, the Quality Control Unit reviews the documentation and determines whether the sample warrants were issued in compliance with laws, regulations, and published procedures.

After a decision is made, a Notice of Findings is sent to the field office stating specific areas of errors, overpayments, or improvements that could be made in their business process. The Notice of Findings may contain health-related, claimant specific information if appropriate.

At the end of each quarter QCDI sends a report to the Disability Branch describing findings at the statewide level. The report describes items such as what caused most of the errors or overpayments in a statistical manner. Information in this report is not claimant specific and does not contain claim detail. There is no privacy impact on this report.

Files containing medical information are locked in filing cabinets. Only QCDI staff has access to those files and the key is maintained by a support staff person. Each analyst keeps working files at their own desks. They each have the ability to lock their cabinets at the end of the day

and have a general knowledge that all confidential information should be kept out of sight and in locked drawers when not attended.

Files may travel outside of the office to analysts' homes on occasion. It is general staff knowledge that files are to be kept out of view of unauthorized persons at all times.

Program Review Branch - Audit and Evaluation Division

The Program Review Branch, Audit and Evaluation Division (A&ED) conducts programmatic audits and case reviews. The A&ED investigates and coordinates prosecution of identified DI program fraud, as well as conducts DI administrative audits.

Policy Development Unit

The Policy Development Unit located in DI's central office is responsible for creation and configuration of all documentation utilized by the field offices. These documents include:

- Disability Insurance Determinations and Procedures Manual

- Disability Insurance Management Handbook

- Claim related forms that go to claimants, medical providers or third parties; i.e., WC or VP carriers

- Non-Industrial Disability Insurance documentation (in process)

- Paid Family Leave Manual and forms

- Other handbooks specific to appeals and overpayments

These individual manuals, forms, and handbooks represent EDD's requirements for policy and business process. All policies and procedures created by this unit correlate to a specific EDD administrative requirement documented in the EDD Administrative Manual. Many policies and procedures from these documents are referenced in the Privacy Gap Analysis document and include privacy specific language regulated by other laws.

Updates for manuals are sometimes issued as DI Notices, which are then amended into the appropriate manual, or are directly made into the appropriate manual. A DI notice is sent out when there is a need to expedite the communication of the policy or procedural change. Direct amendments made to the manual are published as hardcopy documents, as well as updates to the manual on the Intranet. Formal training is not performed for staff for most changes and updates to policy unless it is a significant change in business process. The Policy Development Unit will then prepare and deliver the training, either to every field office and customer service centers or to representatives from each office, who then conduct the training in their office.

Training materials are stripped of any claimant identifying information. The SCDB that is used by claims management and customer service staff has a test database for training but does not use real claims data or claimant-identifying data.

For the most part, medical information is not received in the Policy Development Unit. Appeals staff may get referrals that request appeals elevations. In these cases, the unit will get claim specific information to help assist in the appeals process.

This unit is responsible for adding HIPAA language to the claim form requesting authorization of DI to obtain protected health information from medical providers. The authorization requires a signature by the claimant in order to request, use, and disclose health information.

Human Resources

The Human Resources unit located in DICO is responsible for submitting hiring packages for all DI staff and processing the new employees' paperwork for DICO staff. The Human Resources unit works with all field offices to help office managers with questions regarding corrective action plans, progressive disciplinary action, and reasonable accommodation requests.

Human Resources never obtains information on claimants. Health information is received and stored in DICO for DI employee purposes only and is locked in a filing cabinet. Employee medical information is kept separately from the personnel files.

Voluntary Plan Unit

The Voluntary Plan Unit located in DICO supports employers who decide to provide an alternative to the State Plan Disability Insurance. The forms, processes, and systems for filing a claim all go through the employer's Voluntary Plan (VP).

The Voluntary Plan Unit performs compliance and audit checks on the VP employer in order to ensure that benefits are paid correctly and eligible claimants are receiving benefits. The only health information collected in the Voluntary Plan Unit is for compliance audits and corrective action plans. Voluntary Plan staff visits Voluntary Plan employer sites and reviews claims to see if they are paying or denying benefits appropriately. Copies of claim records are not taken from the employer, but a form is completed by the auditor. The form contains claimant name, Social Security Number, claim effective date (CED), yes and no questions and answers, and comments. No health-related information is collected on this form. If an employer is found non-compliant, then a corrective action plan is created. At this point, the auditor will request that the employer send claim information to the Voluntary Plan Unit. This information is kept in binders filed by year and stored in a locked room. The corrective action plan may require the VP to send medical information to the Voluntary Plan Unit to clear a finding of an overpayment of benefits or a payment issued beyond the medical certification period.

Customer Relations Unit

The Customer Relations unit is located in DICO and receives calls from claimants. Staff from Customer Relations responds to emails and written correspondence received from claimants. Claimant calls represent the greatest number of calls into the Customer Relations unit. Staff within the unit look at the information contained in the SCDB, but do not have access to the paper records but may request a fax of the claim documents from the field office in order to assist the claimant. The information is used and immediately destroyed. The unit may also contact providers to obtain information regarding the claimant. Once the information has served its purpose it is destroyed.

The DIB employees, a claimant, a person with written authorization from a claimant, or a legal representative of the claimant may view the customer file. A claimant, or other authorized person, may send information which is entered into the claimant's records. Information in the

customer file is disclosed on a need-to-know basis. There are different levels of global security access to the systems depending on job function.

<u>Field Offices</u>

Field offices receive, use, and disclose most of the protected health information within the DIB. The Field Offices are responsible for processing disability insurance claims. Claimant medical information is collected initially on the DI claim form. The claimant and doctor fill this form out and either the claimant or the doctor mails it to the CMO. Clerical Support staff enters the information into the SCDB. It is then batched and forwarded to the claims examiners.

Each examiner stores any claims that have not been worked on top of their desks. After the claim has been worked, it is filed in central files by the last four digits of the Social Security Number. The files are not stored in locked filing drawers but the examiners work behind locked doors where there is little availability to the public and generally no access. Family members may be permitted to visit but it is at the discretion of the Field Office Manager.

Appeals are primarily handled in the CMOs. Clerical Support staff pull the original claim information into a file for use in the appeal. This information is transmitted electronically to the Office of Appeals (OAP) of the California Unemployment Insurance Appeals Board (CUIAB) and is also packaged and mailed on paper. A set of copies that is delivered to them is kept at the field office.

The OAP transmits the hearings schedule daily to the field office. The schedule is batched with the files for that day and given to the claims examiner. Most of the hearings are done offsite and vary depending on location of the field office. Copies of the files travel with the claims examiner to the hearing. It is general knowledge and practice that files are returned to the office as soon as possible.

Once the decision is made by the ALJ, the CMO is sent a notice of the decision that may contain medical information. After implementing the decision, the appeals paperwork is filed. In cases where the parties are not satisfied with the decision of the ALJ, they may submit an appeal to the CUIAB.

All claim documents are shredded after the applicable period of time.

4.3 Technical Environment

This section provides a description of the technical environment impacting EDD's systems and infrastructure, including its expected operational life; system interfaces; State and EDD policies; and financial, legal, and public policy constraints. A description of the technical resources and staffing required to support the system is also provided.

4.3.1 Expected Operational Life

The SCDB system is expected to continue operations for the foreseeable future.

4.3.2 External System(s) Interface(s)

Please refer to FSR Section 4.1.9.

4.3.3 Financial Constraints

The EDD must operate efficiently and responsibly. The EDD's executive management has required that the DIAP3 make the most cost-effective use of funds and leverage enterprise resources. The proposed solution must consider the costs associated with the full system lifecycle, including development, deployment, and ongoing costs.

4.3.4 Legal and Public Policy Constraints

The DIAP3 must take into consideration and comply with laws and public policies, and protect HIPAA covered data. The DIB's partners share protected health information which is critical for determining DI eligibility. Additionally, DIB uses sensitive wage data for processing claims, and this information must be guarded from unauthorized access.

4.3.5 Department Policies and Procedures Related to Information Management

The DIB follows EDD's record retention schedule. Claim forms and supporting documentation are kept for a maximum of four years and then shredded. However, claim data is kept in the SCDB system for seven years until it is archived for permanent storage. Additionally, EDD has an Information Security Office (ISO) that sets security policy and practices.

4.3.6 Anticipated Changes in Equipment, Software or the Operating Environment

There are no anticipated changes to the operating system and hardware platform that the SCDB system currently resides on.

4.3.7 Availability of IT Personnel

The Information Technology Branch provides primary support for the SCDB system. There are approximately 52 IT positions dedicated to the support of DI systems. Support of DI systems includes developing and testing new and modified applications due to legislative mandates or changes to the business needs; maintaining applications; building and administering databases; and supporting the on-line CICS environment, desktops, networks, security access, telecommunications, and automated call processing.

4.4 Existing Infrastructure

The existing infrastructure within the larger EDD technology environment consists of the following components:

- **Databases**. The EDD utilizes a variety of database technologies within its environment. The mainframe utilizes IDMS (v15). In the server environment, Oracle and Microsoft SQL Server are used. DB2 in Unix is used for the Base Wage file and PIN systems.

- **Application development environment**. The SCDB application language is COBOL for CICS. The standard application development tool set is EDD's mainframe Programmer Workbench and Change Man. Other application development tools include EasyTrieve, SyncSort, Xpediter, FileAid, AbendAid, and Dial 280.

- **Operating system software**. The SCDB mainframe operating system (OS) is OS390 (v2.10). At the desktop, PCs run on Microsoft NT 4.0. Most servers are either Windows NT or Windows 2000. The EDD utilizes UNIX servers internally and at HHSDC, most of which will be transitioned to Windows.

- **Security**. The current technology environment addresses security on various platforms ranging from MVS (mainframe) using IBM's Resource Access Control Facility (RACF); the mid-range computing platforms (AIX/UNIX and Windows) using server hardening techniques; and the Personal Computer (Desktop) environment which is being tested and migrated to Windows XP. Anti-virus is deployed centrally and locally. On the each local desktop this anti-virus client performs real-time and on demand virus scanning as may be initiated by the customer. Centrally, anti-virus servers are dedicated to remote scanning and detection of infected desktop devices as part of daily anti-virus scanning operations. Exchange e-mail services are provided by HHSDC and include mail content filtering, virus filtering and mailbox anti-virus scans. Firewall and Server Logs are generated but not used to seek out violations of security issues on the network or with applications at this time. The HHSDC provides data center security functions (including, data back-up and off-site storage services, server/system security, multiple Internet DMZs, intrusion detection, router access controls, network utilization and protection from unauthorized use), but there is no regular internal security audit of network activity for DI. HHSDC, through a third party vendor, continuously monitors and logs intrusion attempts or suspicious activity on their network. Ad-hoc discoveries resulting from these activities are referred to the EDD ISO, but regular reports are not provided to EDD staff. The EDD Central Office is a switched environment that affords additional access control and network segmentation. Many field offices use shared networks that currently lack this added level of security; however these field locations will become part of the switched network under the EDD LATA Network Redesign and equipment refresh projects. Websense is running on the Central Office network to restrict Internet site visits under the LATA Network Redesign. Neither the EDD Central Office nor field offices are fully compliant with current EDD employee access control password policy. Although policies and procedures are in places that require passwords and authentication to all areas of electronic data at EDD. However, based on password audits, an estimated 14.5% of network accesses either use a default password or no password for authenticating user access.

- **Network backbone**. The EDD's Central Office IP backbone is comprised of a routed 100 Mbps fiber optic network spanning five buildings in downtown Sacramento. Field offices have access via full or partial T1 lines.

- **LAN and WAN**. The Central Office has high-speed OC3 link to the HHSDC. All field offices are part of a WAN and have a variety of frame relay connections with endpoints at the HHSDC.

- **Internet service providers**. The HHSDC provides EDD's Internet service.

- **Data center services**. Data center services are provided by the HHSDC.

- **Project management**. The EDD has adopted Project Management Institute (PMI) and Institute for Electrical and Electronics Engineers (IEEE) project management policies and practices on its major IT projects. These project management methodologies conform to DOF's requirements for implementing IT projects.

- **Procurement and contracting**. This unit within the Business Operation Planning and Support Division (BOPSD) supports the procurement strategy and contracting of IT services. The unit provides support to request for proposal (RFP) processes.

- **Print and distribution services**. Existing departmental infrastructure for check production includes Formscan Integrity Management System which tracks checks through the print/mail process to ensure a 100% accounting, initiates reprints, and ensures no duplication production runs.

4.4.1 LAN Servers

There are currently 57 LAN servers in place to support the DI program. They are all enterprise servers performing functions that include storage, back-up, domain management, and help desk. All of the servers are networked. The network protocol is TCP/IP. In addition to the LAN Servers, the PFL program utilizes 16 servers to support its program. There are four PFL Servers in each of their production, training, testing, and development environments.

4.4.2 Network Protocols

The network protocols are TCP/IP. Figure 4-14 depicts EDD's IP network backbone.

Figure 4-14. The EDD Network Backbone
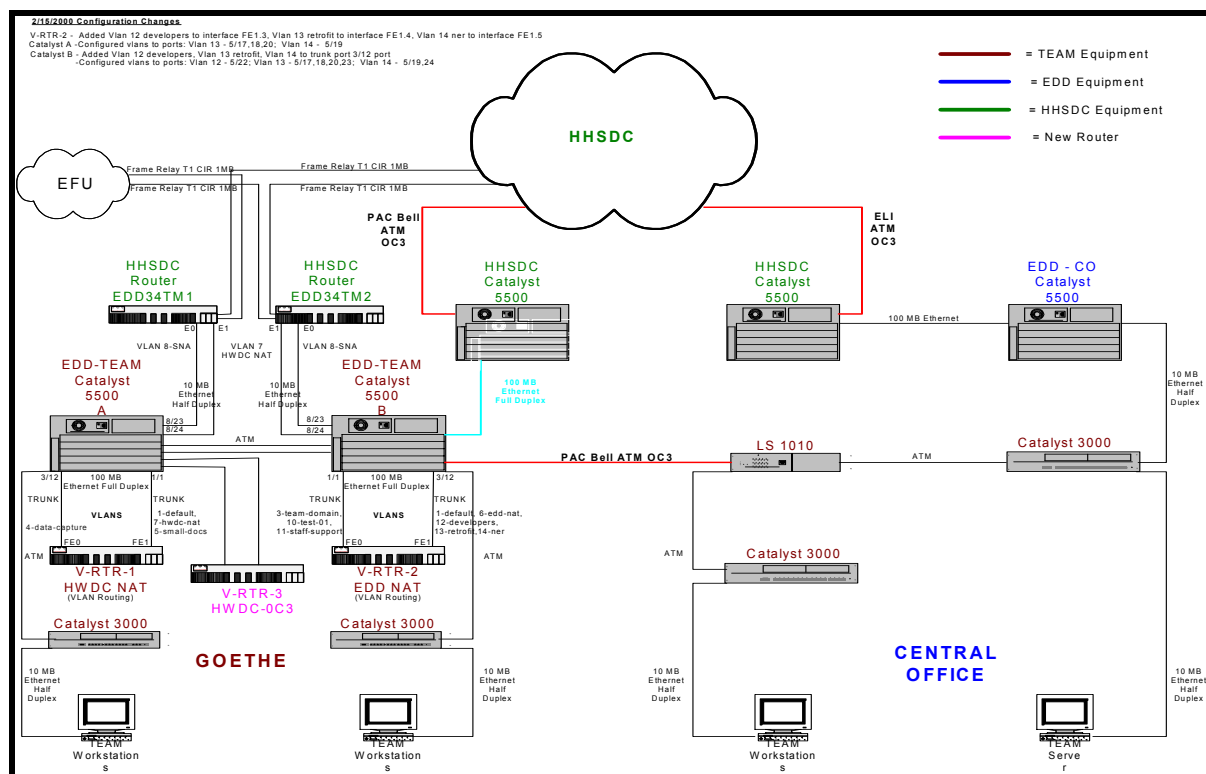
5.0 PROPOSED SOLUTION

The foundation of the DIAP3 solution is the implementation of a secure electronic communications and information processing environment that promotes efficiency and reduces costs by following HIPAA regulations and guidelines. HIPAA affords DIB an opportunity to realize the advantages of electronic communications with claimants, medical providers, and employers.

The DIB intends to undertake a business-based procurement to solicit technical solutions from vendors. Once a proposal is accepted and costs are finalized, DIB will complete and submit a Special Project Report (SPR) to DOF describing the proposed solution, scope of work, and costs.

The DIB believes the business-based procurement approach provides the best opportunity to acquire an automated solution. It will allow vendors the freedom to propose creative solutions based on their knowledge and experience. The business-based procurement approach was chosen for several specific reasons, including:

- Final HIPAA rules have not been approved for two of the unique identifiers (providers and health plans) and for enforcement procedures. If finalized in time, DIB would like to consider the technical requirements for these three rules as part of the DIAP3 solution.

- Likewise, complete HIPAA compliance for covered entities is still in progress and, as such, best practices, tools, and techniques are continuing to be developed. COTS products and packaged solution components related to HIPAA are evolving and competition among vendors is increasing, driving prices down while improving quality. The business-based procurement will allow systems integrators to propose combinations of business and technical solution components that best address the DIB problems and opportunities in this FSR, including cost reductions. Examples include COTS software to validate HIPAA TCS compliance and documentation templates for HIPAA privacy and security policies and procedures.

- DIAP3 will follow the Microsoft .NET Framework and technologies that are part of the PFL IT solution, currently being implemented within EDD. Together, DIB and ITB are solidifying their technical skills and system support strategies on the PFL project. A business-based procurement will allow EDD to re-examine DIAP3's technical and resource requirements prior to release of an RFP, taking advantage of the knowledge and expertise being built on the PFL project.

- The solution will follow the Service Oriented Architecture (SOA) structure currently being planned within EDD. The DIAP3 solution's technical needs in relation to SOA will be finalized by ITB and DIB working in cooperation with the vendor developing the DIAP3 RFP.

- The business-based approach will also permit DIB to re-evaluate the impact of any EDD network or security infrastructure changes that may be in place at the time of RFP development.

The following FSR sections provide summary information regarding solution options that may be considered by vendors in meeting DIB's objectives for DIAP3:

5.1   Potential Solution Description

5.2   Rationale for Potential Solution Selection

5.3   Alternatives Considered

5.1 Potential Solution Description

The potential solution selected for proposed DI Automation Project Phase 3 (DIAP3) incorporates proven technologies with established EDD IT systems and resources. It meets applicable HIPAA requirements and addresses numerous business issues that have emerged over the past few years, as outlined in FSR Section 3. The solution promotes efficiency, establishes reliable applications, and improves business operations.

5.1.1 DIAP3 Overview

Working with a procurement assistance vendor, EDD will use a business-based procurement approach to select a systems integrator (SI) for the DIAP3 solution. An independent verification and validation (IV&V) vendor, independent project oversight (IPO) consultant, and project management consultant will also provide assistance to the EDD DIAP3 project team. The EDD and project team and vendor staff will be subject to EDD confidentiality policies and HIPAA privacy and security requirements, and will be required to sign form DE7410, Confidentiality Statement. The EDD personnel and vendor teams will work together to implement the DIAP3 solution, including new business processes, intake methods, software applications, and databases.

5.1.1.1 New Intake Methods

Currently, key data entry (KDE) of paper documents is the only intake method for DI claims. By the fifth full year of the DIAP3 potential solution's operation, DIB believes new intake methods will reduce key data entry from 100% to a single-digit percentage by implementing the following:

- **Direct electronic interface** for medical providers to submit claimant health information in a highly secure, HIPAA-complaint manner to DIB, using the Internet.

- **Intelligent forms** for claimants, employers, and medical providers to electronically submit DI claim information through the use of the Internet. It will provide claimants and employers with easier and more efficient access to DIB and will also offer individual or small medical providers another secure method to submit claimant health information.

- **Image-scanning/OCR** technology to convert remaining paper-based claims to electronic format. Paper claim forms will be redesigned for intelligent character recognition so that most paper claims will be accepted as scanned. Exception processing will identify claims that require manual processing. KDE will remain as an intake method for the exceptions identified in the scanning/OCR process. Industry statistics indicate that exceptions are minimal. The need for scanning will decrease as direct interface and intelligent forms gain widespread use.

- As part of the intake process, DIAP3 will use **automated workflow** to manage the routing of incoming documents from intake to appropriate claims examiners, and through each step of the claims determination process.

Figure 5-1 illustrates DIB's evolution to an electronic data environment.

Figure 5-1. Evolution to Electronic Data
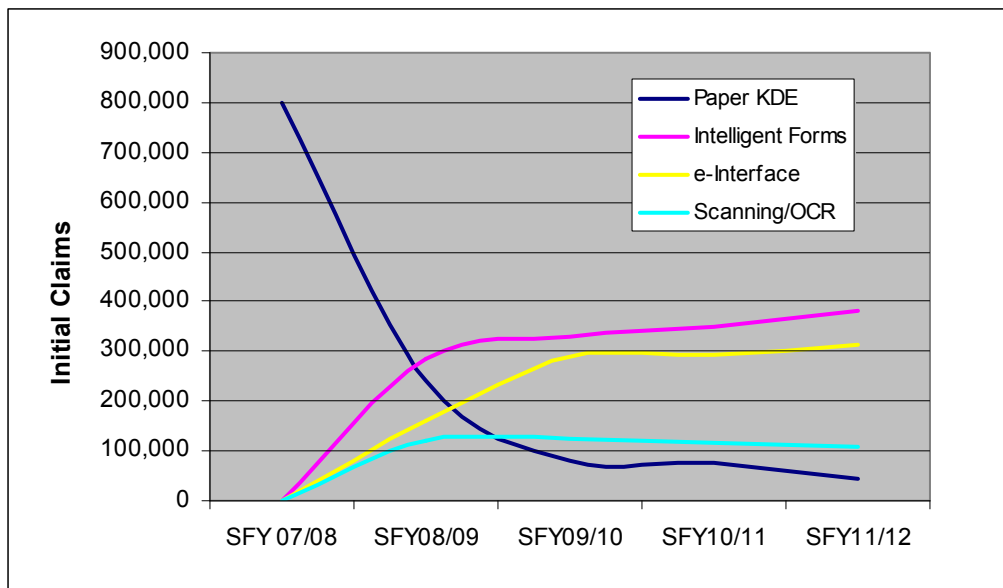
Both the e-interface and intelligent forms methods are expected to significantly reduce the processing of paper once they are put into place. For any remaining paper claims, scanning/OCR will be implemented to convert these documents into electronic format. For purposes of preparing this FSR, DIB's preliminary strategy includes rolling out the new intake methods in phases, with the direct electronic interface and intelligent forms first, complying with medical providers' HIPAA requirements and making that part of DIB's business more efficient. Implementing these two methods together will facilitate the matching of the claimant portion of the DE2501 with the medical provider certification portion of the DE2501.

The direct e-interface, intelligent forms, and scanning/OCR intake methods will interact with new Web-based applications and with the SCDB using a Service Oriented Architecture (SOA) structure. The matching process will be part of the business logic in the new .NET applications. However, other solution implementation timing and features may be proposed by SI vendors. The selected solution must minimize changes in the SCDB itself, extend the life of EDD's investments in its legacy systems, and stay within the bounds of EDD IT standards.

Direct Electronic Interface

Most of DIB's medical provider business partners have already complied with HIPAA regulations and implemented secure information systems that allow them to collect, protect, and transmit PHI electronically in a fully HIPAA-compliant manner. The DIB will create direct (business-to-business) electronic interfaces with its large medical providers so they can submit claimant

health information to DIB in a HIPAA-compliant manner. The direct interaction with medical providers and partners will increase over time and reduce the volume of paper processed.

To indicate the scope and potential economies provided by direct interfaces, Kaiser Permanente, DIB's largest medical provider, is responsible for medical certification on approximately 25% of DIB's initial claims volume in some geographic areas, and 14.3% of initial claims statewide. In SFY 03-04 this amounted to 109,000 medical provider form pages. Moving the current paper-based process to an electronic process is estimated to save DIB approximately 4 claims processing staff annually for Kaiser-certified claims alone.[10]

The first direct business-to-business interface in the DIAP3 solution will be with Kaiser Permanente, who has expressed an interest in working with DIB. The direct interface will then be expanded to other large medical providers. The medical providers will send data in the HIPAA-compliant ANSI X12 format, and DIB will accept and store information in a claimant electronic file folder.

Data received over the direct interface will be processed by new .NET applications, and will first be stored in the SQL Server database. The new applications will link the medical providers' claim data with claim data that claimants will submit either through intelligent forms, scanning/OCR, or key data entry.

Intelligent Forms

Several vendors have developed suites of COTS products that support intelligent forms functionality. Intelligent forms use common, open standards such as XML and PDF. Large medical providers use XML extensively in their automated, HIPAA-compliant environments. In effect, the technology removes the key data entry tasks from DIB employees and assigns them to the claimant, medical provider, and employer. Intelligent forms minimize the need to process paper and copy information from paper into automated systems.

Web-based intelligent forms will provide claimants, medical providers, and employers an alternative to hardcopy claim submission. The forms are "intelligent" since they can automatically verify that required information is complete before allowing submission, perform mathematical computations within the form to fill calculated fields, and transfer repeated data from one page or form to another (such as company name, ID number, address). Intelligent forms will improve DIB's review efforts by eliminating the need to check routine calculations and basic filing information.

Intelligent forms deliver virtual images as XML documents that can be stored, retrieved, and archived electronically via the Internet, reducing the need for paper storage and management, and speeding the transfer of legally acceptable documents between DIB locations. Attached documents can be included with the forms to support claim submissions. In addition, intelligent forms allow secure digital signatures either through the use of native digital signature technology or in conjunction with third-party digital certificate authorities such as Verisign, Entrust, or RSA.

---

[10]Estimated SFY 03-04 initial claims volume of 763,350 times 14.3 percent, times a savings factor of 3.87 minutes equals 422,466 minutes divided by 60 equals 7,041 hours divided by 1,725.9 (EDD's PY factor) equals 4.08 PYs.

Intelligent claim forms will decrease the number of errors submitted while simultaneously reducing the manual and redundant workload placed on the medical providers, employers, and claimants completing the forms. The technology provides greater data integrity by providing user prompts, screening out potentially incorrect data, and reviewing the claimants' data against acceptable criteria. Additionally, the forms provide the claimant with the ability to check the status of their claim over the Internet, potentially reducing the number of calls to DIB's CSCs.

Upon submission into the DIAP3 solution, intelligent forms and new business logic will allow additional validation, comparison with other data elements, and system updates. Using intelligent forms and the DIAP3 solution, claims meeting predefined criteria would be automatically paid without any additional interaction.

Scanning/OCR

DIB anticipates that once the direct e-interface and intelligent forms intake methods are in place, submittal of paper claims will decline significantly. However, due to the demographics of claimants, paper claims will never be entirely eliminated. To meet the need to efficiently manage paper claims, DIB will centralize the flow of remaining paper by directing it to a scanning/OCR services provider. Mail will be automatically opened and scanned, and the OCR process will capture and validate the data. The document images can be indexed and stored at EDD on a storage area network.

Scanning and imaging technologies will reduce the time it takes to perform key data entry tasks by claims examiners and clerical staff. The DIB will retain required documents electronically and shred paper documents 30 days after receipt. Scanning/OCR will increase staff productivity, reduce facility document storage costs, reduce the cost of reproducing and mailing claimant information among DIB facilities throughout the State, and reduce the risk that accompanies reliance on hardcopy documents. Program staff throughout the State will have online access to both the data and the scanned images of the DIB claim forms. The storage duration, media, and access will be identical to the PFL project. The costs for GTO setup and processing will be re-estimated after vendor solution proposals are received. The records will be stored for four years and if there is no activity on that claim, the records will be purged. The media is "magnetic-disk based records storage." The cost to the PFL system has been limited to the original purchase of the SAN and so far the volumes have been less than expected. The Department believes the costs of the storage platters are nominal. Also SAN storage is much less expensive than the current platter structure by TEAM. The cost for image storage is approximately $17,878 per million documents.

Currently, the Tax Branch's Goethe Tax Operations (GTO) does not have the capacity for the scanning and OCR workload associated with this project. The EDD is currently projecting that DIAP3 scanning/OCR will be outsourced. At this time, outsourcing is an available and cost effective option. At the time the SPR is prepared, EDD will re-evaluate the costs and efficiencies of outsourcing the project's scanning/OCR versus using EDD's GTO facility and services.

Workflow

DIAP3 will implement automated workflow to manage the linking of related claim information, the routing of incoming documents from intake to appropriate claims examiners, as well as through each step of the claims determination process. Workflow logic will also be used to

prioritize claims based on predetermined criteria. This will allow DI claims examiners to focus on claims that require human intervention.

The following diagram illustrates the intake of data via new processes that include direct electronic interface, intelligent forms, and scanning/OCR. Automated workflow will then route data to the new Web-based application environment where it will be evaluated, standardized, and either sent to the mainframe SCDB or new SQL Server for storage.

Figure 5-2. DIAP3 Proposed Solution Overview
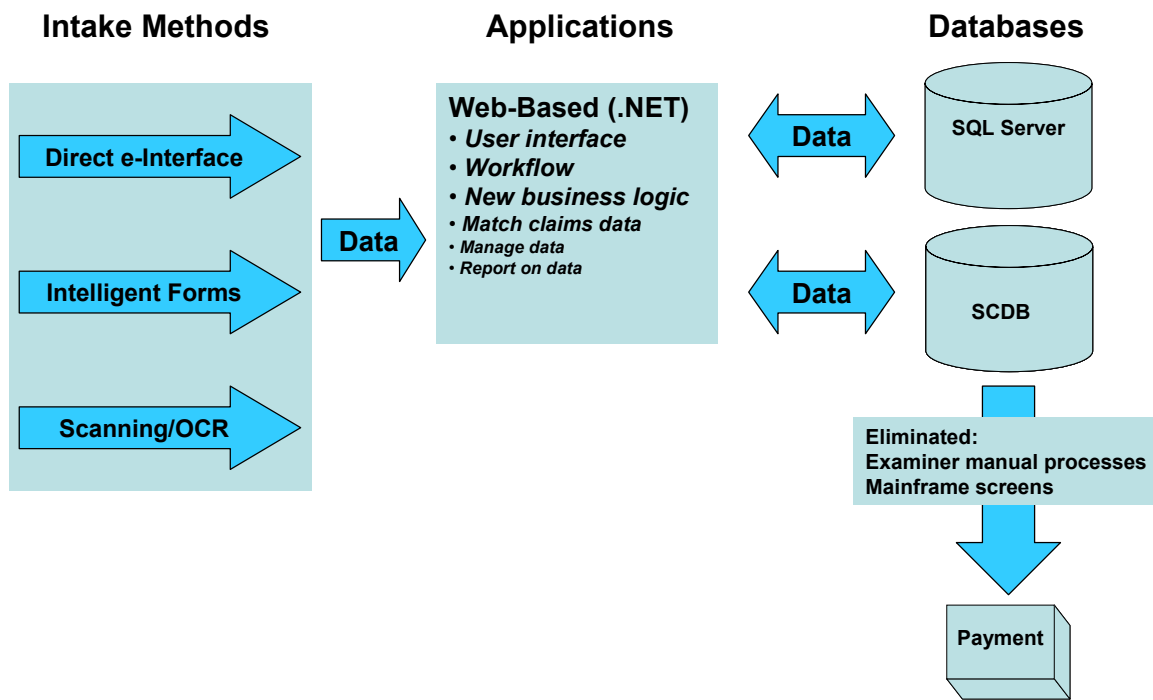
5.1.1.2 Foundation of Secure Electronic Communications and Applications

This potential solution implements HIPAA-compliant electronic communications as its foundation. Secure e-communications are fundamental to all HIPAA regulations, rules, and guidelines. Examples of DIB-specific requirements include:

- Encryption of DI transmitted data, device, and media controls development

- Improved inventory procedures for IT assets and e-PHI

- Information transmission security enhancements throughout the EDD network

- Data integrity

- Use of digital signatures for authentication

- Enhancements for facility access control

- Access terminations for automated sessions

- Security awareness training and security incident reporting

- Contingency plan development/revision

Implementation of HIPAA-compliant secure electronic communications will reduce risks and vulnerabilities to a reasonable and appropriate level and further safeguard DIB against unwanted activity by internal and external entities.

Claims Management, Work Flow, Financial, Program Integrity, and Decision Support Applications

New applications will provide DIB with flexible, responsive, and scalable business processing tools that will allow the organization to automate a number of business functions now being performed manually. For purposes of costing in this FSR, the project's software development environment will be a Web-based framework using Microsoft's BizTalk Server with business rules and process orchestration engines, as well as .NET for Web services and component software.[11] .NET applications run on Intranets as well as public Internet sites. .NET is an all-inclusive Web-oriented software architecture for internal and external use.

The .NET/BizTalk applications will support new intake methods and contain business logic to automate DIB's manual processes and populate required fields in the SCDB. New application functionality will include:

- Claims Management

- Workflow and Document Management

- Financial Management

- Program Integrity

- Decision Support

Information from the intake methods will use the .NET/BizTalk architecture and SQL Server database for storage and retrieval to enable collection, review, claims matching, and correction of data before it is transferred to the SCDB. Additional data not currently captured in the SCDB will also be stored in the new SQL Server database. The new system functionality will generate new data elements that will need to be stored, similar to the PFL system. New functionality contributing to the new data elements is in the areas of Claims Management, Workflow and Document Management, Financial, Program Integrity, and Decision Support. The reason these new data elements will be stored on the SQL Server Database and not SCDB, is to maintain consistency with the architecture already established with PFL, and to leverage to the degree possible the existing PFL hardware/software. One Time costs for SANS is $180,000, with four SQL Server Enterprise licenses at $15,000 each. PHI data will be protected by a number of methods.

The .NET/BizTalk applications will invoke existing online mainframe programs to read and update the SCDB. This environment will allow:

- Online entry of claim requests by claimants via the Internet/Intranet browser

---

[11] .NET is Microsoft's approach to a comprehensive development and runtime environment similar to Sun's J2EE (Java 2 Platform, Enterprise Edition) platform for building distributed enterprise applications.

- Online and automatic eligibility determination

- Automated claim payment generation and distribution

- Online access to claimant electronic case file from any DIB location

- Acceptance of secure HIPAA compliant X12 electronic data feeds of PHI from medical providers

- Acceptance of digital signatures

- Online claim modification

- Sharing of data electronically with dissimilar systems

- Performance metrics and alerts via an interactive digital dashboard tailored specifically to the DIB environment

- Extensive reporting capabilities

Although SI vendors will be able to propose details regarding their plans to implement a DIAP3 solution, its applications will automate DIB's business processes in five primary areas, as shown in Table 5-2.

Table 5-2. The DIB Proposed Solution Application Suite

Module	Description of Functionality
Claims Management	The objective of this application module is to create an electronic file folder that will introduce new automation to DIB's claims processing functions. The module will automate most of the claims data intake and filing functions. New business logic contained in the system will assist in: processing new claims, processing exceptions, making eligibility determinations, tracking medical provider information, and tracking employer-related information.
	Enhancements will also upgrade claim computation and recomputation capabilities, notification of normal expected durations for disabilities, determination of payment, establishment of overpayment, maintenance of overpayment records, updating claim information, and the processing of appeals. The system will also associate all claims-related correspondence (referred to as "white mail") in an electronic file folder.
	The new functionality will allow DIB claims examiners to more efficiently track all of the information in a claim electronically and act upon it quickly and efficiently with a wide range of system prompts and built-in logic. The claims management functionality as envisioned in this module and in use in similar case management systems creates a cascade effect of efficiencies that simplifies the overall processing of claims workload.
Workflow and Document Management	The new system will associate all claims-related information in an electronic file folder. The system will allow the user to retrieve one or all of the documents associated with a claim. It will also provide the capability to queue these files to designated DIB staff without regard to location. This capability will allow DIB management to balance workload among statewide staff.

Module	Description of Functionality
Financial	The new system will trigger and pass through all of the current system's critical financial computations as well allow DIB to develop new, more efficient ways to utilize and build on this information. The actual financial payment of the claim will be done by the legacy system. Added financial features in the proposed solution are aimed at managing the case of a claimant, providing a way to store, track, and review financial information more effectively, and, as such provide opportunities to detect and prevent fraud and abuse. The functions are anticipated to include automatic update of claimants' records to reflect the benefit disbursement and automated comparisons to assist in preventing fraud.
Program Integrity	The reduction of fraud and abuse is a major element of both HIPAA and DIB's business goals. The program integrity module addresses fraud detection and assists in the investigation of fraud and processing of audits. This module puts in place new functionality that will assist DIB in combating fraud by augmenting DIB's current fraud deterrent and detection capabilities, practices, and tools and adds additional functionality in the areas of fraud detection and quality control.
	Functionality provided by this module includes the ability to flag claims for further review if they fit certain fraud parameters. Other functionality includes the capability to track medical providers with a past history of fraud, allowing the Field Office Integrity Specialists (FOIS) to leverage existing fraud reports, and make notes in the system regarding a file. The system will also automatically select a random number of claims for quality control review.

Module	Description of Functionality
Decision Support	Decision support technologies will be implemented to gather, store, and analyze data to help enterprise users make better business decisions. This solution module will include querying and reporting, online analytical processing (OLAP), statistical analysis, forecasting, and data mining. Also referred to as business intelligence (BI), these tools will assist DIB management with numerous daily, weekly, and monthly reports as well the capability to generate complex ad hoc reports regarding DIB's claims and claims processing workload. It will improve DIB's ability to identify, classify, and intelligently analyze all available information. Decision support functionality will be used for several types of decisions: • Operational decisions, helping the DI Branch operate efficiently – for example, based on the triggers that cause a claim to be tagged for human intervention and the results of the actual human interaction with the claim, how can the validation rules (or other system features) be modified to gain additional efficiencies? • Tactical decisions, helping to determine alignment with objectives – for example, what is the trend for initial claims requiring intervention over the past 6 months? 12 months? How does this trend compare with expectations for implementation of the new system? • Strategic decisions, helping to make sure the organization and new system are keeping pace with change – for example, how many key data entry positions are projected to be needed in the next fiscal year? What is the impact of shifting workload from one office to another? Currently, system-generated reporting is inflexible and limited, and the data is generally historical rather than up-to-date. Decision support needs are met primarily through high-level reports, institutional knowledge, and information gathered in discussions and meetings. Lacking real-time data to make decisions, DIB will not be able to measure the effectiveness of its operations across all areas, including detection and prevention of fraud and abuse. Real-time reporting and access to information is critical to streamlining the enterprise and improving customer service.

5.1.1.3 DIAP3 Team Members

The EDD staff will work with vendors to accomplish DIAP3 goals and facilitate knowledge transfer—both EDD to vendor and vendor to EDD. The DIB and ITB staff will be heavily involved in the design, development, and implementation of the project to support self-sufficiency in on-going maintenance and operation of the system.

Several methods of checks and balances will be used to help ensure successful completion. Per EDD policy, a project oversight consultant will be brought on to the project first. The project oversight consultant will monitor the project, identify potential risks, and provide support for reporting. A procurement assistance vendor will help develop the RFP and provide technical

expertise to the evaluation team to assess proposals of Systems Integrators (SIs). The IV&V vendor will validate compliance with technical and functional requirements and alignment with HIPAA throughout the SI contract period. The IV&V vendor will be instrumental in ensuring that all aspects of DIAP3 are properly tested before being deployed. A project management consultant will be selected to work with EDD's project manager and the SI in scheduling the various tasks and activities involved in the project. The PM consultant will also assist with project reporting and issue management.

5.1.2 Solution Structure

The solution will follow the Service Oriented Architecture (SOA) structure currently being planned within EDD. The EDD SOA is a layered architecture, with the Data Layer at the bottom. Other layers generally build on top of each other with the Presentation Layer at the top of the stack. Communications are initiated to layers equal to or lower in the stack than the originator.

Figure 5-3. SOA Overview
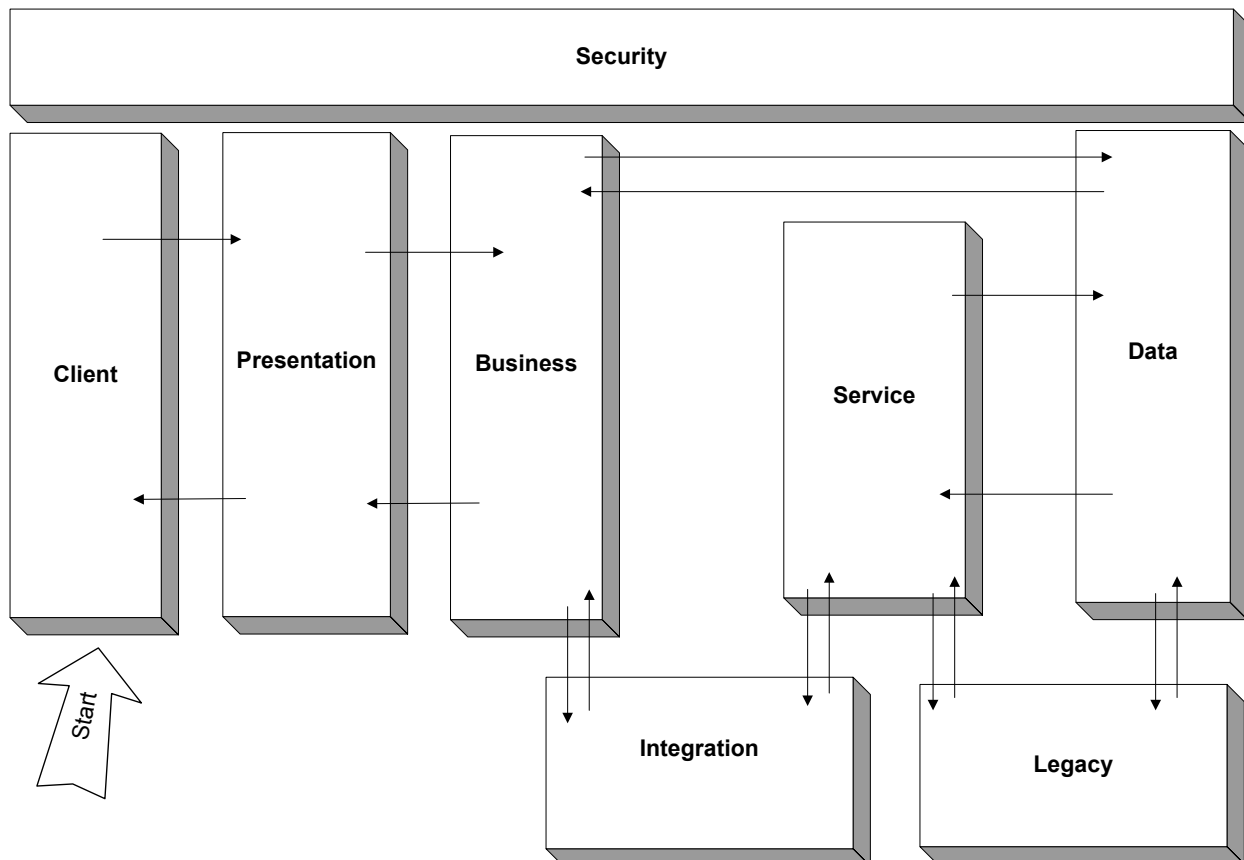
5.1.2.1 Data Layer

Beginning from the bottom of the stack, the Data Layer is made up of two sublayers:

- Data Storage Sublayer—houses the actual DBMS, such as the IDMS SCDB

- Data Access Sublayer—abstracts out the data access functionality, and is responsible for making and handling the actual calls to the database, as well as packaging the results of database access into an XML document. The data access sublayer acts as a virtual database in that it appears to be a single data source to its clients, but it acutally synchronizes multiple physical databases.

The SCDB will remain the primary data repository in the potential solution. Since it is used extensively by other EDD branches as well as by DIB, it will not be restructured, which would a time-consuming, risky, and very costly endeavor. A SQL Server database will be used as a storage and retrieval staging area, for data to be collected, reviewed, and corrected. Data that can be stored in the SCDB will be transferred there. Other data will be stored in the SQL Server database. For any given logical grouping of data (domain object) request, the Data Access Controller will determine why physical data to read/write from the SCDB and/or from the SQL Server database, and assemble it into/from an XML document representing the target domain object. This will then be passed to the requestor.

Figure 5-4. Data Layer
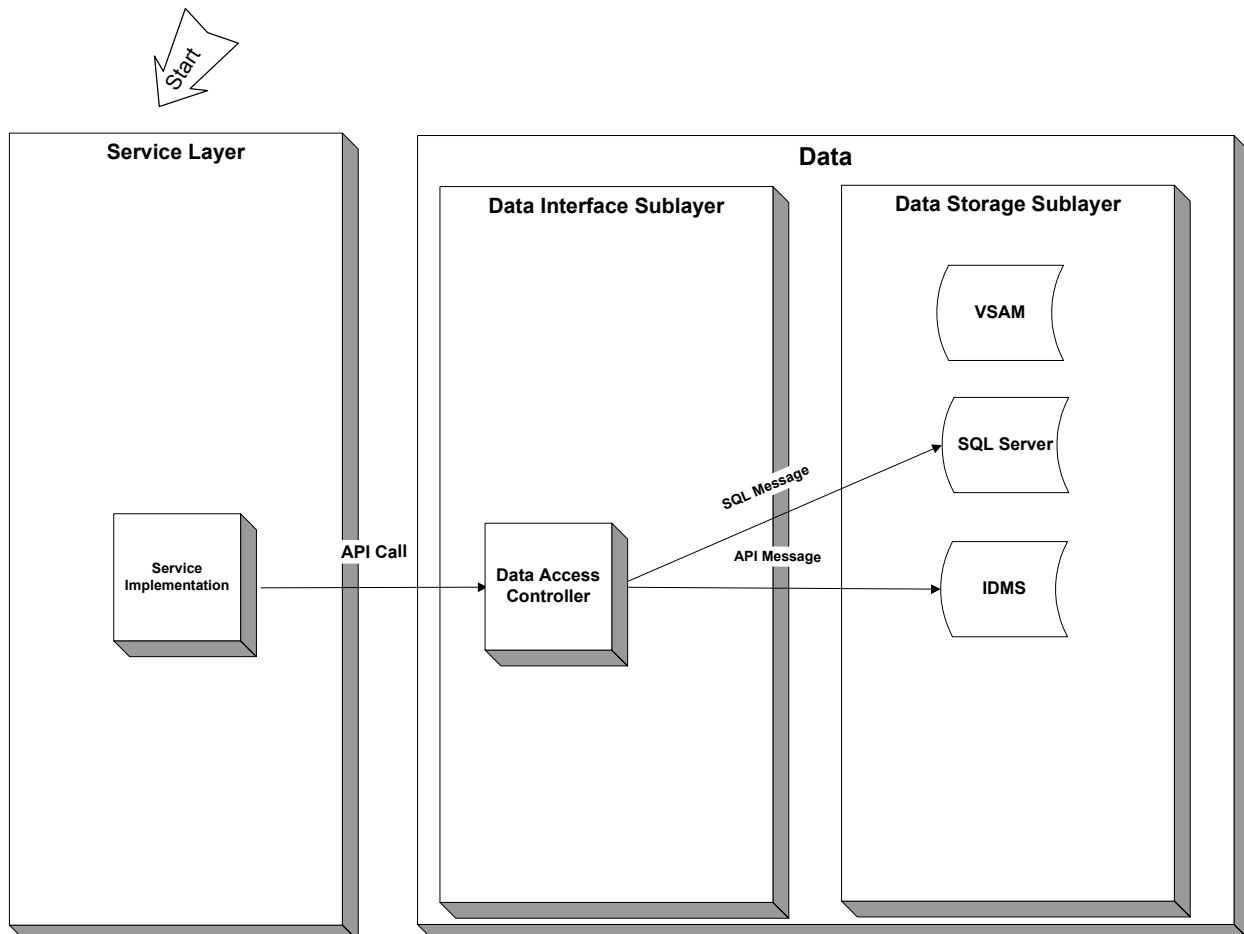
5.1.2.2 Legacy Layer

The Legacy Layer is the next higher layer, and is comprised of two sublayers:

- Legacy Access SubLayer—abstracts out the legacy access functionality, and is responsible for making and handling the actual calls to the legacy programs, and for reformatting and packing the results into XML documents that are returned to the requestor.

- Legacy Program Sublayer—houses the actual CICS-COBOL programs

The Legacy Access Controllers will be responsible for implementing an interface consisting of a set of logical data requests by accessing multiple legacy programs, reading relevant data, and packaging it into an XML document for return to the caller.

Mainframe applications in the Legacy Program Sublayer will continue to provide functionality. CICS-COBOL screens will be scraped to collect data which will be written in XML format and exchanged with other layers. The new DIAP3 .NET applications in the Business Layer will trigger the legacy systems to perform computations. The legacy applications will be modified as needed to interface with the DIAP3 system. The new functionality will reside in the new parts of the system.

Figure 5-5. Legacy Layer
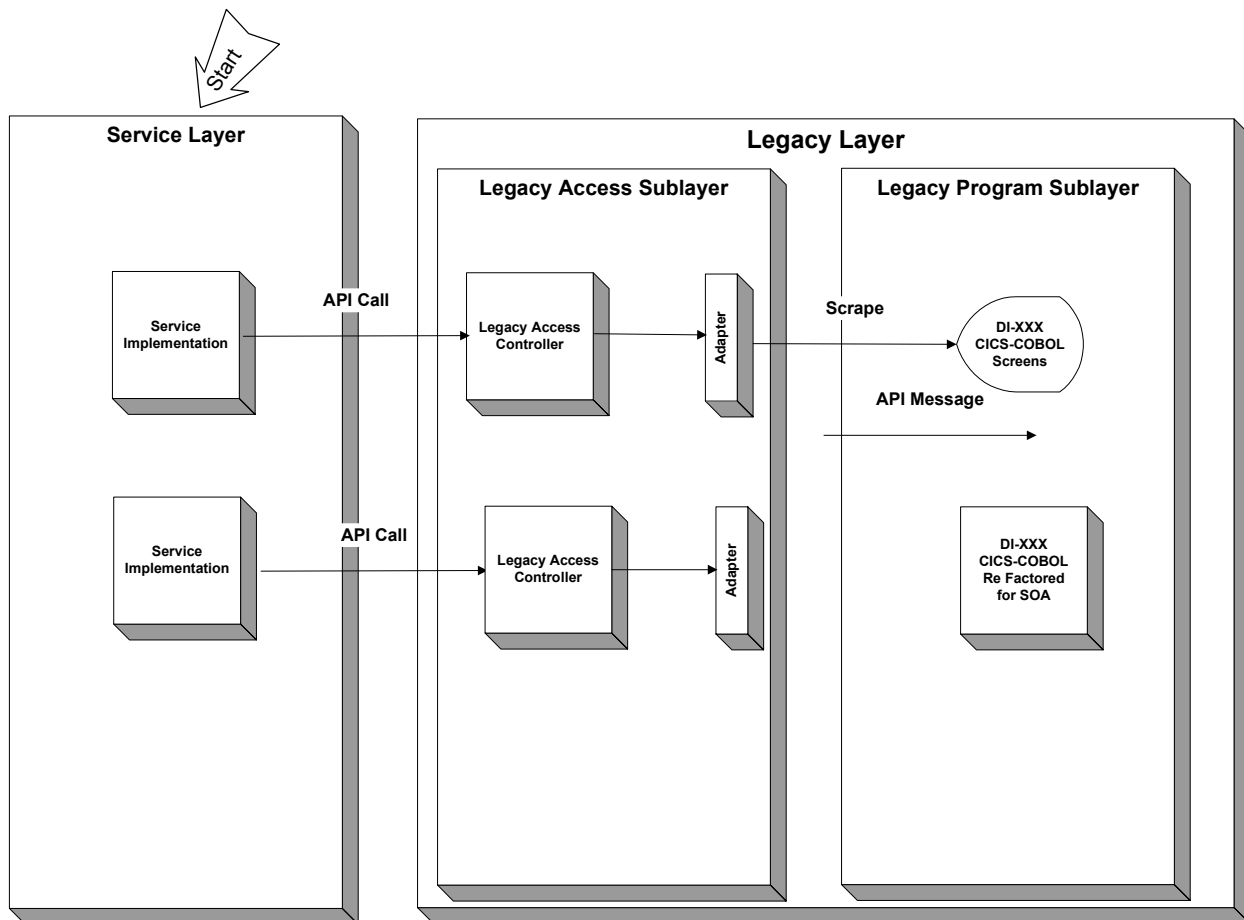
5.1.2.3 Service Layer

The Service Layer sits between the Data Layer and Integration Layer and houses the components that implement the services. Services sends and receives Simple Object Access Protocol (SOAP) messages, which contain an XML document for information exchange. Services connect to the Integration Layer endpoints and are accessed via the integration server. A security sublayer sits between the Integration and Service Layers, and applies authorization security to all service calls.

Figure 5-6. Service Layer
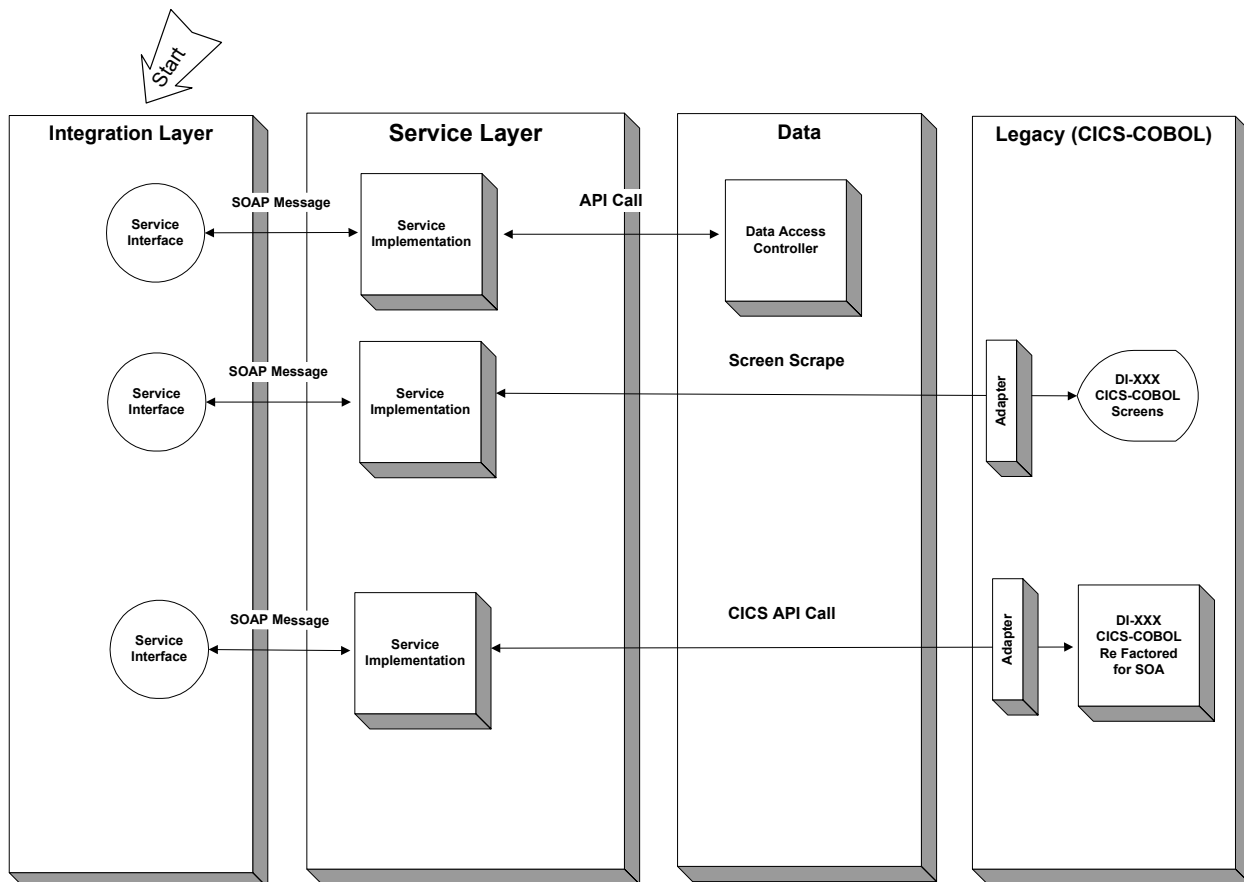
5.1.2.4 Integration Layer

The Integration Layer hosts the BizTalk Integration Server which abstracts out interfacing with services, as well as message routing and delivery between services, orchestration of services into business processes, application of routing and business rules. Applications and services connect to the integration server at endpoints which supply the attached applications with a standard set of services, as well as access to any other service connected to the integration server. One of these important services is adapting the protocol of the calling application to an EDD-standard XML data format. This EDD-Standard XML, which should reflect industry standards and business partner vocabularies, is used in communicating with endpoints throughout, and when reading/writing data to the Data Access Sublayer.

The Integration Layer includes automated workflow to efficiently route messages in an appropriate manner and apply business rules. It also houses a process orchestration engine that abstracts out the routing and sequence rules of a business process and facilitates the building and running of compound services.

Figure 5-7. Integration Layer
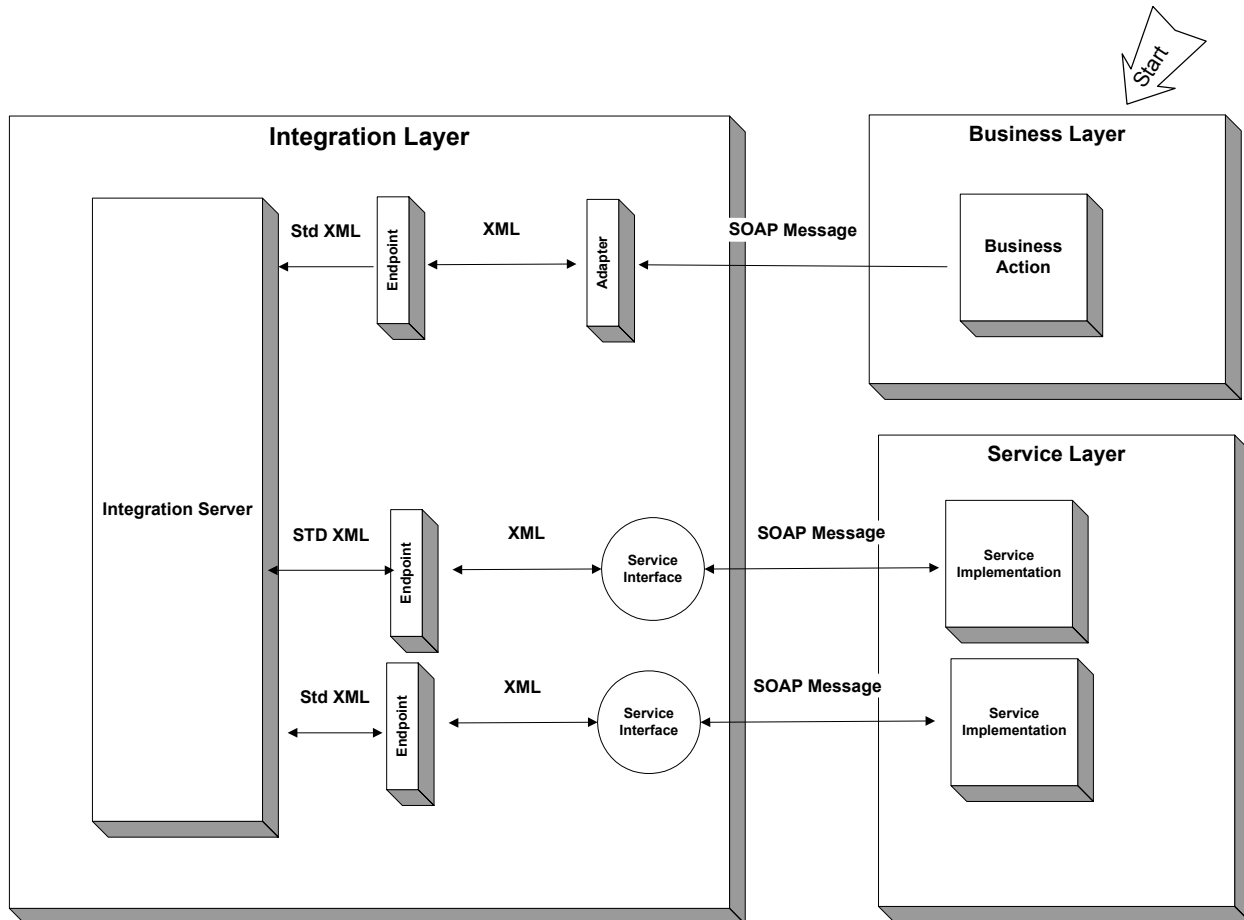
5.1.2.5 Business Layer

The Business Layer hosts the Business Action objects. Business Actions represent a single business function, and implement a common interface in order to be interchangeable from the viewpoint of the caller, facilitating easy application configuration. The Presentation Layer is the layer in the stack immediately above the Business Layer, and is responsible for determining which Business Action to call. The Business Action can either delegate some or all of its responsibilities by attaching to the integration server at an endpoint and calling upon services to do the delegated work. It can also do all of its work and data access itself.

Figure 5-8. Business Layer
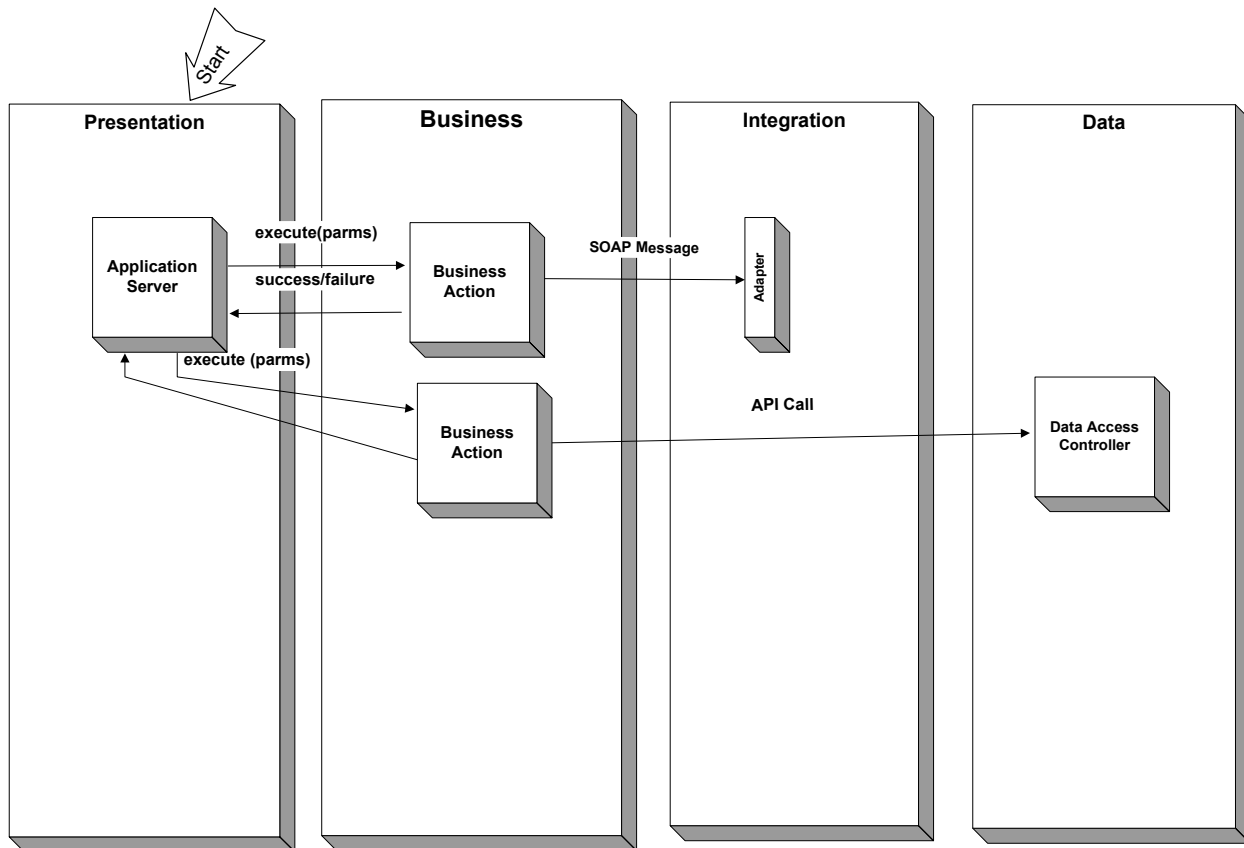
5.1.2.6 Presentation Layer

The Presentation Layer will manage new intake processes that offer alternatives to submitting paper-based claims. DIAP3 includes replacing the existing DI mainframe-based 3270 data entry screens with a new user interface.

The Presentation Layer will receive HTTP requests from clients and send HTTP responses to clients. A Security Layer will intercept all requests and apply authentication. Submitting a screen with an intelligent form will cause an XML document to be automatically generated from the form, containing the data and processing instructions wrapped in the HTML request. This layer will forward HTTP requests from Web servers to application servers for processing where appropriate. It will also determine the next navigation action to take based on the results of executing the business action.

The Presentation Layer will:

- Give medical providers the ability to directly transmit claim information electronically to DIB in HIPAA-compliant XML document format.

- Permit online, Internet submittal of DIB intelligent forms claim requests by customers and allow for the dissemination of these forms electronically to all DIB locations.

- Automate the input of paper-based forms at a central intake facility.

Figure 5-9. Presentation Layer
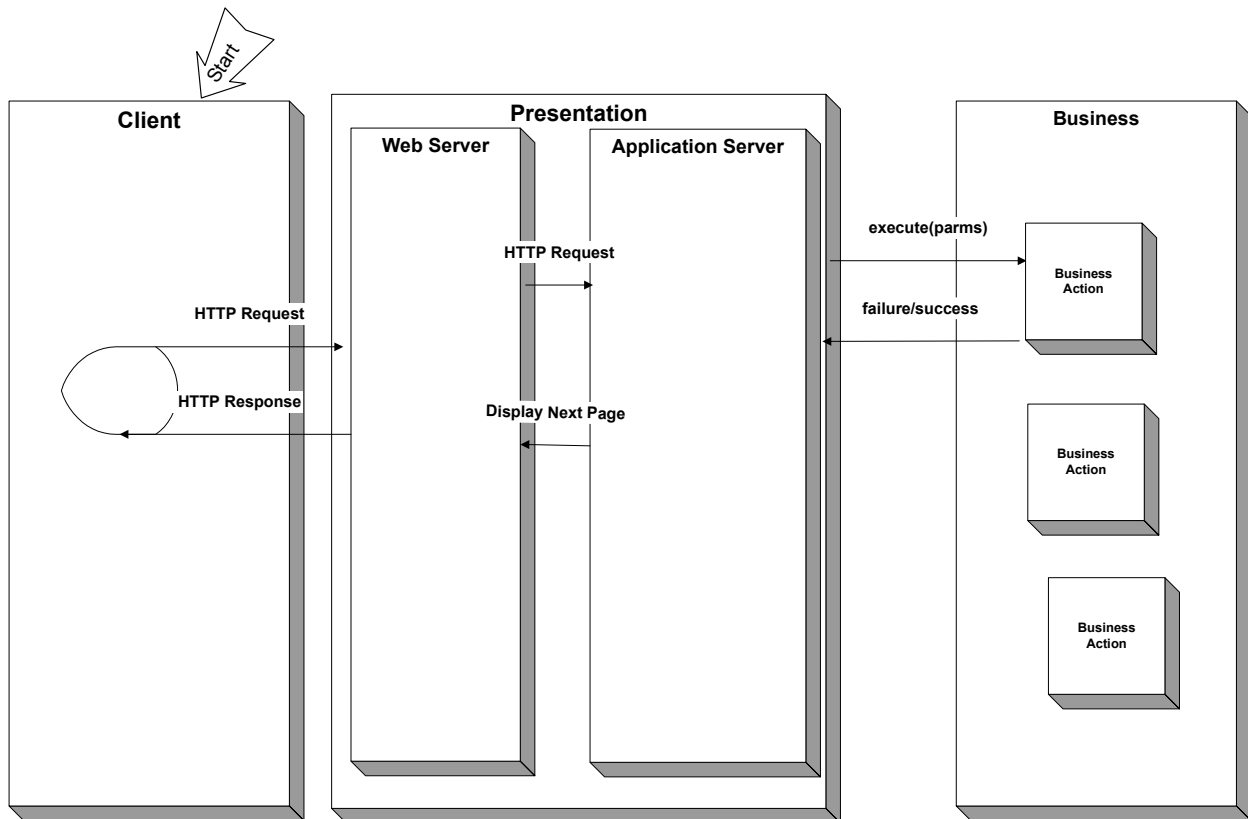
5.1.3 Hardware

All hardware will comply with EDD server standards and operations policy. Servers will be configured in a clustered format to provide fault tolerant operations and housed at an EDD location, with the exception of the intelligent forms servers, which will be at a State data center. DIAP3 requires purchase of a storage area network for scanning/OCR, personal computers, and servers, as follows:

FY 2006/2007:

- PCs for new staff, 6 at $2,065 each for a total of $12,390. Includes 1 year of warranty and 2 years of maintenance.

FY 2007/2008:

- 19 additional PCs for new staff. $2,065 each for a total of $39,235. Includes 1 year of warranty and 2 years of maintenance.

- 17 production, test, development, and training servers at $30,000 each for a total of $510,000. (Note: There may be additional capacity in the DI servers being used for the PFL program. If capacity is available, the number of servers for DIAP3 will be reduced)

- 1 server with added magnetic storage RAID array for decision support, $45,000.

- $100,000 in hardware for Tivoli Access Manager for e-business (TAMe).

FY 2008/2009:

- 4 additional PCs for new staff. $2,065 each for a total of $8,260. Includes 1 year of warranty and 2 years of maintenance.

- $180,000 for scanning/OCR image storage device, storage area network (SAN).

5.1.4 Software

DIAP3 will use existing as well as new software. The DI-specific application server portion of the potential solution will utilize the Microsoft .NET framework. The architecture contains a Web server that processes HTTP requests and responses; an application server that provides business functions, thread management and database connectivity services; and a database server, which provides data storage and access. All software purchases as anticipated in FY 2007/2008 and include:

FY 2007/2008:

- Intelligent forms software estimated at $1,047,680.

- $50,000 in XML utility/tools for development of the direct interface.

- Security-related software totaling $104,000 ($50,000 for encryption products, $50,000 for audit/correlation tools, $4,000 for policy/procedure template suite).

- $100,000 in decision support software.

- $39,000 for 15 licenses for Visual Studio .NET, based on per seat license of $2,600.

- $150,000 for messaging gateway software to transfer information from the mainframe to the Web-based environment.

- $52,000 for SQL Server.

- $100,000 in Tivoli Access Manager for e-business (TAMe) software.

- $25,000 for BizTalk Server software.

5.1.5 Technical Platform

The technical platform is Microsoft's .NET framework. Microsoft's .NET architecture is comprised of the following three basic building blocks:

- PCs, laptops, workstations, telephones, handheld computers, tablet PCs, and other smart devices that have the ability to access XML-enabled services.

- A core set of building blocks that perform routine tasks and act as the backbone for development by Microsoft and third parties.

- .NET Enterprise Servers, including the Microsoft Windows 2003 server family and BizTalk Server, make up the Microsoft .NET server infrastructure for deploying, managing, and orchestrating XML-based services.

Potential solution technical requirements are listed in FSR Appendix E.

5.1.6 Development Approach

The EDD explored several alternatives for DIAP3 development. The primary business drivers of the development approach are the HIPAA mandates which require HIPAA-covered entities to comply with Privacy, Security and Transaction and Code Set regulations.

The DIB will contract with a systems integrator to design, develop, and implement the DIAP3 solution. Contracts with IV&V, project management, and oversight contractors will support the project. The development approach also takes into account that a coordinated business process analysis and re-engineering effort must be taken to ensure that the electronic direct interface and intelligent forms work with the image-scanning environment and that the technologies support each other.

The EDD will use an internal software development methodology for changes to the DI and supporting applications. The systems integrator will be expected to adhere to this development methodology as well, which is based on IEEE standards and the Rational Unified Process. The new functionality will be developed using Microsoft's .NET architecture and delivered through a combination of in-house and contracted support. The development and testing approach will incorporate EDD's standards and tools.

The development approach includes sufficient attention to implementing business processes related primarily to new intake methods and new applications. The SI vendor will provide change management, marketing, and business process reengineering services.

5.1.7 Integration Issues

Implementing the DI intake and output processing requires new internal systems integration between the e-interface, intelligent forms, current DI applications, the scanning/OCR vendor, and SCDB. The systems integrator will be responsible for ensuring that the systems successfully inter-operate.

5.1.8 Procurement Approach

The DIB will use the procurement approach outlined in Table 5-4.

Table 5-4. Procurement Approach

DIAP3 Purchase	Solicitation Type	Procurement Schedule	Contract Start-End
Procurement assistance vendor	CMAS	04/2006 – 06/2006	07/2006 – 08/2007
Independent project oversight consultant	CMAS	04/2006 – 06/2006	07/2006 – 06/2009
Independent verification and validation vendor	IT MSA RFO	04/2006 – 06/2006	07/2006 – 06/2009
Project management consultant	CMAS	04/2007 – 06/2007	07/2007 – 06/2009

DIAP3 Purchase	Solicitation Type	Procurement Schedule	Contract Start-End
Systems integrator	Multi-step Formal RFP	07/2006 – 06/2007	07/2007 – 06/2009

The procurement assistance (PA) vendor will be procured using CMAS, and will be tasked with assisting DIB and DGS' Procurement Division (DGS/PD) in undertaking the business-based procurement. The PA vendor will review and revise DIAP3 functional and technical requirements and incorporate then into a Request for Proposal (RFP). Vendors will be invited to participate in a multi-step formal bid process, submitting Conceptual, Draft, and Final Proposals. The PA vendor will provide documentation support throughout the acquisition process. Additionally, as the SI begins its contract, the PA vendor will continue to provide support, transferring knowledge to the IV&V vendor.

Per EDD policy, the IPO consultant will join the team at the beginning of the project, and be tasked with monitoring and reporting support functions. The EDD will work with DGS/PD in using the IT MSA to procure an IV&V vendor, who will provide services throughout the SI vendor's contract. The PM consultant will be chosen using a CMAS solicitation, and will support scheduling and tracking for the project.

The DIB considered other procurement approaches, including separate procurements for:

- Mainframe connectivity
- Direct interface development
- Intelligent forms solution
- Security vendor(s) services
- Business intelligence/decision support
- IV&V
- Project management/reporting
- Marketing
- Training
- Equipment
- .NET infrastructure implementation
- DI applications design/development
- Direct electronic interfaces
- Application testing
- Deployment

The complexity of many individual purchases, as well as the level of effort required to ensure the successful outcome of a cohesive solution made this approach unacceptable.

5.1.9 Technical Interfaces

Technical interfaces will be the responsibility of the SI vendor. The DIAP3 applications will require an interface provided by the mainframe messaging gateway to enable communication between the .NET environment and the mainframe. DIAP3 intelligent forms will also require an interface to the .NET platform and SCDB.

5.1.10 Testing Plan

The systems integrator will create the Test Plan for approval by the IV&V vendor and EDD project management. Testing of the DIAP3 solution will require EDD and the vendor to plan, execute, and complete both unit and system testing with input from the IV&V vendor. System testing will include load and performance testing to ensure that the implemented system can meet data volume and concurrent user requirements. Acceptance testing will cover appropriate HIPAA compliance needs (especially security), and include reliability and functionality testing, printing, workstation access, application access, and testing of backup and recovery procedures.

The ISO and A&ED will be involved in testing. Regression testing will be performed on DI, TAS, and BAS applications to ensure that changes made for the DIAP3 do not affect current processing. The testing process will be conducted in accordance with existing EDD test standards and procedures, and approved by the EDD project manager and the DIAP3 Steering Committee.

5.1.11 Resource Requirements

The proposed solution requires the addition of new EDD IT staff and vendor assistance to either augment State staff or provide skills that are not available in State staff. Various EDD resources will be involved in the project, including but not limited to most DIB teams, ITB, ISO, UIB, and A&ED. Costs for the proposed resource requirements are detailed in Section 8, Economic Analysis Worksheets.

Contractor resource requirements include:

- An independent project oversight contractor to assist with risk and issue monitoring and reporting.

- An IV&V vendor to assist in the procurement of the SI and provide validation of the design, development, testing, and deployment of the technical solution.

- A prime systems integrator to provide software design, development, testing, and implementation services.

- A project management consultant to support the IT Project Manager in scheduling and tracking day-to-day project tasks, activities, milestones, and deliverables.

The proposed solution costs are detailed in Section 8, Economic Analysis Worksheets.

5.1.12 Training Plan

Training additional EDD IT staff on .NET and programmatic integration components of this solution is a key component and is required to initiate and support the system. Technical training for IT staff will address the development, maintenance, and user administration skills to support the system. The SI vendor will also provide a Knowledge Transfer Plan that documents how the vendor will ensure that State staff receives the knowledge and training to support the new application and technical environment after implementation and deployment is completed.

The EDD DI Program will develop a Training Plan that will outline the strategy and approach for training DI staff on the new functionality. DI end-user courses will be conducted throughout the State at various facilities and computer-based training will be provided where possible.

5.1.13 Ongoing Maintenance

The proposed solution requires on-going maintenance hardware and software, EDD labor costs for system operation and maintenance, and data center services. Details of the costs can be found in Section 8, Economic Analysis Worksheets.

5.1.14 Information Security

The business requirements for HIPAA compliance document the confidentiality and security needs for the automated systems. The following summarizes the main points:

- Compliance with the IT standards required by HIPAA and EDD
- Authentication of users
- Access protocols
- Data integrity
- Audit trail for all system activities and events
- Encryption

Existing EDD information security will be augmented. With the use of Internet/Intranet applications, the possibility exists of confidential data being accessed unless encryption of PHI is fully implemented throughout DI systems. Encryption of confidential data must be addressed and included in the selected solution. Encryption is for e-PHI in transit, within the EDD statewide network and specifically for information between DI and external insurance and medical partners (such as independent medical providers). No encryption is planned for the SCDB.

The proposed solution includes security levels implemented with layers of servers and other protections to adhere to the following requirements:

- Appropriate firewall solutions will continue to be used
- Audit trails will be provided
- Information stored on the DIB Automation Project and SCDB databases will be accessible to authenticated users only

- Each user will be assigned to one or more user communities, depending on the profiles established for the user community

- The proposed solution will support different levels of local and statewide access

- Encryption – all transmission of electronic files will be encoded as well as transmission from database

- All personal and PHI-related data will be stored in encrypted format in each production database

Security roles, access levels, and privileges should be based on DIB business function and managed by the user login and authentication process. These access levels may include:

- Inquiry

- Additions

- Deletions

- Modifications

- Security maintenance (e.g., creation or update of security profiles)

- System maintenance (e.g., table-driven system parameters)

All database transactions will be logged, ensuring data accountability for the actions of any individual as follows:

- Every system event will be logged under the user's name

- After a user is logged on and working, the system will keep track of all data accessed, entered, and modified

- Whenever data is viewed or reviewed, the individual who last accessed, entered, or modified the data will be identified

- Each screen will be individually controlled

- If a user is logged on but does not actually use the system for a defined period of time set by policy, the system will log the user off

- Users will be asked to reconfirm their identify if the system has been left idle for a period of time defined by the EDD security policy

- Pursuant to the California Civil Code, the Information Practices Act, audit trail logs will be retained for a minimum of three years. For e-PHI access control and log records, per the HIPPA Standard 164.312(b), Audit Controls, and the EDD will plan to adopt this standard.

5.1.15 Confidentiality

Data stored in the new DIB application will be highly sensitive and confidential in nature. Information, as required by law and/or regulation, may be shared with other authorized entities outside the immediate EDD environment. Therefore, the proposed solution will include comprehensive security features that support the capability to:

- Limit access to specified users and/or units based upon the confidentiality of information

- Limit access to confidential data

- Limit access to selected applications, screens, and/or data based upon user security identification

- Limit access to specified users and/or units based on organizational structure

5.1.16 Impact on End-Users

The following are the major program and process impacts that the potential solution will have internally on DIB staff, and also on the DIB Program stakeholders.

For DIB staff:

- It will minimize key data entry.

- Navigation of the DIB application for claims examiners will be easier via the use of electronic file folders.

- Processing of routine claims activity will be automated.

- Incomplete documents will be automatically rejected and routed for correction.

- Automated integrity alerts to claims examiners will provide improved fraud detection and stop loss processes.

- Workload will be balanced and distributed by automated transfer of workload to other DIB offices, and then between claims examiners.

For medical providers:

- It will improve business relations by making it easier and more flexible to do business with DI, by accepting information in formats that they use, and providing several ways for them to submit information.

- It will assure the security and privacy of personal information submitted to DIB.

- It will minimize opportunities for fraud at intake, during claim processing, and internal to DI.

- It will separate the medical provider information submission from the claimant's.

- It will assure accurate identification of medical providers submitting information electronically.

For claimants:

- It will help ensure that benefits are not delayed or prevented.

- It will provide an electronic alternative, via online or Web-based intelligent forms, to filing paper claims.

- It will assure the HIPAA-compliant security and privacy of the personal information submitted.

- It will provide faster access to claims processing information.

For employers:

- It will provide an electronic alternative, via intelligent forms, to providing and receiving DIB paper forms.

5.1.17 Impact on Existing System

Impacts to the DI mainframe system are categorized as follows:

- **User interface.** Currently the DIB clerical and claims examiner staff must manually key claim data into the legacy DI system. Under the new system, claim data will be captured via intelligent forms, direct interface, and document image scanning. The claims information will be uploaded into the SCDB for further processing. No changes to the SCDB user interface layer are expected.

- **Application logic**. DI applications currently manage the other DI business functions and internal processes. The existing messaging gateway must be configured to allow access to SCDB claims processing, payment authorization, check and form printing, and accounting services from the .NET environment.

- **Data management**. The SCDB and ABAS include all financial transactions, claimant and claims information, eligibility, and other data. The DIB will not require the addition of any new fields or records.

The components of the potential solution were selected because they leverage and would not have a negative impact on the existing systems and programs. In effect, the proposed solution extends and builds upon existing systems to accommodate DIB's requirements and position EDD for the future. The impact to existing systems is minimal, including modifying the mainframe system to process claims and checks and implementing decision support software to collect data elements.

5.1.18 Consistency with Overall Strategies

Leveraging existing technologies and reducing impact to existing programs meets EDD's overall strategies. Further, the proposed solution is aligned with the mission and vision of EDD and supports the cost minimization initiatives outlined by the State.

5.1.19 Impact on Current Infrastructure

The solution leverages existing EDD standards and technologies where possible without the risk of making major changes to the mainframe system and impacting other programs. Some infrastructure additions will be required since technologies such as intelligent forms and direct interface with medical providers will be implemented.

5.1.20 Impact on Data Centers

The solution will minimally impact State data centers. SCDB ongoing support will remain the same.

5.1.21 Data Center Consolidation

The intelligent forms servers will be housed at a State data center.

5.1.22 Backup and Operational Recovery

Because this project is built by extending current, in-place systems, the backup and operational recovery requirements will be founded on existing plans. In addition, appropriate procedures for the backup and recovery of the DIB intelligent forms servers and .NET-based application and server environment will be implemented by EDD in conjunction with the SI vendor.

5.1.23 Public Access

The proposed solution allows and encourages self-sufficiency as a means of improving customer service. Claimants, medical providers, and employers will have various avenues to access information relative to their needs online or via the existing interactive voice response system.

Each avenue will have specific security technologies, consistent with EDD security standards, to ensure that individuals accessing the system are both authenticated and authorized to submit and retrieve information. PIN/password, electronic signature, and security tokens are examples of methods that may be applied as appropriate. Data will be encrypted per HIPAA standards before transmitting personal health information, or data that is otherwise considered confidential or sensitive. To ensure ongoing security, the system will allow for comprehensive monetary review and investigational audits of user access, automatic notification of access irregularities, and the ability to analyze trends in user access.

5.1.24 Costs and Benefits

As detailed in the Economic Analysis Worksheets in Section 8, the total one-time implementation of the potential DIAP3 solution is estimated at $25 million. Continuing costs for the project are $3 million/year. Savings are primarily reductions in staff that process paper claims.

The DIB believes the reductions are at a pace that can be achieved through normal attrition. In FY 09/10, DIB will require 80.1 fewer PYs than estimated in the existing baseline. For FY 10/11, the decrease through attrition year to year is 79.7 PYs when comparing FYs 09/10 and 10/11. Likewise, for FY 11/12, the decrease through attrition year to year is 60.4 PYs.

The DIB expects the following benefits from the selected solution:

- Enables DIB to follow HIPAA regulations for privacy, security, and transactions and code sets

- Allows DIB to implement HIPAA administrative simplification directives

- Eliminates the negative impact on claimants when medical providers delay completion of certification forms or assess extra charges for manual forms completion

- Provides more avenues of access to DIB for claimants, medical providers, and employers

- Creates more efficient systems and processes

- Improves program integrity, reduces fraudulent activity

- Leverages existing EDD standards and technologies without the risk of making major changes to the mainframe system and impacting other programs

- Adheres to EDD technological vision and builds on current EDD technology initiatives

- Maximizes the use of internal IT resources while contracting for additional services to meet restrictive implementation timeframe

The project will:

- **Implement a secure DI system.** The proposed solution expands existing technology functionality and information contained in the SCDB system and leverages existing security infrastructure, including HHSDC firewall and network security provisions within HHSDC and EDD. The solution also protects all DI data in compliance with Information Security Office (ISO) and the EDD's enterprise security solution, for internal and external security.

- **Support DIB's business partners so they can comply with applicable HIPAA mandates.** The proposed solution enables DIB to provide security and administrative simplification functionality required by its business stakeholders who are HIPAA-covered entities. Key functionality that will be part of this implementation includes protection of claimant health information, claim processing, claim payment, audits and fraud detection, appeals, overpayment determination, fiscal workload tracking, and benefit accounting.

- **Optimize the use of DI claims processing staff.** The proposed solution utilizes existing EDD Enterprise processes and support infrastructure to provide timely benefits to claimants. It leverages existing document management functionality and technologies within EDD to support initial claim data intake and management of extended claims. Data sharing between EDD's business areas and its customers and stakeholders is improved and key data entry of claims information is reduced by using intelligent forms, optical character recognition (OCR), and intelligent character recognition (ICR) processes and technologies. Operational risk is mitigated by digitally storing information, removing organizational reliance on paper documents.

- **Minimize operational costs.** The proposed solution minimizes operational costs because it is supportable by EDD's technical staff in IT operations and application maintenance. Furthermore, it is consistent with EDD technology direction and industry technology trends and direction.

5.1.25 Sources of Funding

Funding for the DI Automation Project Phase 3 will come from the DI Fund. Continued funding for this project will be provided through the DI Fund.

5.2 Rationale for Potential Solution Selection

The potential alternative addresses DIB problems and opportunities, as well as meets DIB's objectives and requirements. The DIAP3 will speed the flow of work, improve work quality, and provide management with far more detail and metrics upon which to base decisions. The highly flexible and scalable architecture will allow DIB to quickly build new applications in a HIPAA-

compliant secure telecommunications and operations environment. This flexibility will enable DIB to better respond to mandated future changes. The proposed solution:

- Utilizes the SCDB for common reusable processes and functionality.

- Builds upon DIB's Microsoft .NET distributed computing platform for deploying HIPAA compliant electronic communication internally and with external stakeholders, including HIPAA compliant X12 transaction formats.

- Evolves DIB's paper-based claims processing to an electronic environment that includes automated workflow technologies.

- Replaces many manual claims processing tasks and business operations with new software applications.

- Implements secure, Web-based application environments consisting of interrelated components that will protect DI's business partners' HIPAA-covered PHI and provide DIB with a highly flexible, scalable, and industry-standard IT platform.

- Fulfills DIB's chain-of-trust responsibility to its business partners who must comply with HIPAA regulations.

- Improves claimant, voluntary plan provider, medical provider, and employer access to DIB services.

- Strengthens EDD's network security and implements new technologies in alignment with enterprise IT standards.

The solution is fiscally responsible and risk averse, taking into account the merits of sound planning and vendor expertise in new technologies, supporting project development in collaboration with EDD IT resources. The Web-based applications and other technologies will allow for direct submittal of claims in a secure computing environment, complying with HIPAA. The Web-based .NET framework is an open architecture that is scalable and easily accommodates change, laying the groundwork for the future functionality. .NET includes EXtensible Markup Language (XML) and numerous Web services protocols such as ANSI X12 and ASC X12, supporting the implementation of HIPAA -mandated standards.

In summary, the potential solution introduces new technology solutions while taking advantage of existing DIB mainframe functionality. The use of existing EDD technology will minimize cost and risk. The proposed new DIB data intake staging and data output functionality will be developed in a .NET environment using a relational database. This approach avoids a major database restructure of the SCDB and adheres to departmental strategic direction for new application development. It also fits with EDD's IT projects and their strategic direction.

The proposed solution meets all of the objectives and the corresponding requirements defined in Section 3, *Business Case.* It conforms to EDD and DIB strategic business and information technology plans.

It provides a cost-effective solution that minimizes the need for clerical staff, cuts DIB operational costs, and reduces fraudulent activity. Furthermore, Gartner research shows that it is imperative for IT organizations to develop and execute an object-oriented migration strategy to transition away from traditional legacy architectures. Implementation of the proposed solution complies with EDD's IT Strategic Vision, while meeting project and program objectives in a cost-effective and timely manner.

The proposed potential alternative assumes that existing technology architecture and investments will be utilized. It relies on and leverages the existing security infrastructure, including HHSDC firewall and network security provisions within HHSDC and EDD. It enhances and expands the organization's security-related infrastructure and operational policies.

With the successful implementation of the proposed solution, DIB will ensure continued business operations with its covered entity partners, and will achieve its strategic objectives in administrative simplification—improved customer access to services, increased electronic communication with trading partners, and integrated data access within the Disability Insurance Program. Most importantly, it will ensure that claimants continue to receive their disability insurance benefits in a timely manner and with no disruption due to HIPAA compliance issues.

5.3 Other Alternatives Considered

A number of potential alternatives were considered by EDD to ensure that all possibilities were explored. Research uncovered two viable alternatives, as well as a number of other alternatives that were excluded. Prior to thoroughly analyzing the viable alternatives for automating DIB, a brief description of other alternatives deemed inappropriate is provided. The excluded alternatives were:

- Procuring a commercial off-the-shelf (COTS) case management application to support DIB's operations

- Obtaining an automation solution from another state

- Maintaining the status quo

A market survey was conducted to determine if there were any COTS applications that could meet DIB's array of needs. Although the research indicated several portal products targeted to Disability Insurance carriers were available, the functionality of these applications was very limited and did not meet DIB's needs. The survey did not find any COTS case management systems built specifically for organizations like DIB.

Only four other states and one Commonwealth (Rhode Island, New Jersey, New York and Hawaii, and the Commonwealth of Puerto Rico) offer a state-administered disability insurance program. Only Rhode Island and New Jersey's programs are similar to California's program. New Jersey's system does use image scanning as a component, but does not utilize OCR for data capture. Additionally, a survey conducted during the HIPAA Gap Analysis indicated that they were either using mostly manual processes (like DIB), had old technology, or utilized non-scalable applications that would not support DIB workload volumes.

The DIB could elect to do nothing and live with the current system with its many complex manual processes. This would put DIB in an untenable position with its business partners by being non-HIPAA compliant, further drain the State's finances through continuance of inefficient and wasteful practices, and be in direct contravention of the new administration's executive orders (particularly Executive Order S-5-04) to make the State's departments and agencies more accountable, responsive, and efficient.

This alternative would prevent EDD from meeting the applicable federal HIPAA guidelines as well as DIB's mandated legislative requirements and is, therefore, not considered viable. It is presented in detail to establish the current baseline for the economic analysis worksheets.

5.3.1 Alternative Description

The EDD considered one other viable alternative in addition to the proposed solution to meet the business objectives and functional requirements of the solution. This alternative is described below and a brief assessment is included detailing costs, benefits, recommendations, and reasons for exclusion.

EDD is one of the largest organizations of its kind in the world. The work volume of its UI, Tax, and Disability Insurance Branches process is larger than the volumes of many other states combined. Until recently, the only IT environment capable of dealing with these huge work volumes was the mainframe environment. Over the last few decades, EDD has developed an extensive mainframe-based IT infrastructure and knowledgeable support staff, and as noted earlier in this report, modern applications to fit DIB's requirements can clearly be developed in a mainframe environment. As a result, development of DI automation in the mainframe environment is a technologically viable alternative.

The mainframe-based DI automation initiative includes development in a mainframe environment, restructuring the SCDB, modifying existing DI systems to handle new DI functionality and data, implementing intelligent forms technology, implementing a direct interface with medical providers, and implementing image scanning with OCR/ICR capabilities. The IT staff requirements for the solution were developed by reviewing technology requirements. The solution relies heavily on new in-house and vendor resources. The EDD in-house estimates were compared with experiences to date on the PFL Project, which has similar functionality.

As discussed in Sections 3 and 4, DIB's manual operations are supported by an old mainframe-based system that was developed over 20 years ago and was built in what is now considered third generation technology. The third generation started roughly in 1964 with the IBM System/360. The DIB's medical provider business partners are currently using fifth generation technology.

For the purposes of understanding this alternative, it should be noted that DIB's problems are not a result of the mainframe computer environment, but rather with the now obsolete software architecture and unstructured methodology used to develop the original SCDB application that runs in the mainframe environment. For the purposes of this review, note that the software architecture encompasses the design of the application and component system software that incorporates protocols and interfaces for interacting with other programs as well as the EDD/HHSDC enterprise environment.

The State (more specifically EDD, HHSDC, and DIB) has a very large investment in mainframe hardware, software, and supporting human resources. With more than $2 trillion worth of mainframe applications in place nationally, mainframes are not going to go away, and their centralized architecture, which is the easiest to manage, has some analysts claiming that mainframe development may be the wave of the future. Thus, developing new functionality in a mainframe environment is certainly a technologically viable alternative to consider. Another factor to be considered is that mainframe software and available middleware[12] have evolved in the last two decades. Therefore, a case could be made to restructure the SCDB and rebuild DIB's required applications in a mainframe environment using modern software architecture and

---

[12] Software that functions as a conversion or translation layer. It is also a consolidator and integrator.

a structured development methodology. This discussion assesses the costs and benefits of this approach.

This alternative consists of the use of mainframe hardware resources, a modern mainframe software architecture consisting of IBM's DB2 Universal Data Base (UDB) Relational Database Management System (RDBMS) and IBM's WebSphere Web-based application server products. In the mainframe environment, DB2 is the leading RDBMS and IBM's WebSphere product is generally considered the standard development framework for providing the type of Web-based functionality that Microsoft's .NET applications framework provides in mid-range systems. WebSphere is a family of Web application server products from IBM that run on OS/390, OS/400, NT and various Unix platforms.

5.3.2 Evaluation of Alternative

In an effort to determine the level of effort and costs involved in developing a restructured mainframe solution, the FSR analysis estimated the effort utilizing two standard software cost estimate methodologies. These included: (1) a structured analysis methodology for software development suggested by the IEEE's Computer Society, which has developed standard processes to estimate software development, and (2) a method the federal government favors - the Constructive Cost Model(COCOMO).[13]

The analysis team broke the labor elements into eight categories, estimated the number of hours associated with the level of effort required, and costed the categories by position. All hardware, software, and telecommunications costs were also reviewed as well as ongoing hardware and software costs. The eight major labor components with roles, estimated positions, and hours to complete the work are found in Appendix F.

The alternative would require a major restructure of the SCDB to add the DI-specific records needed to administer the program. The SCDB has not been restructured for 5 years for several reasons. It is a lengthy, expensive, and technically difficult undertaking. It would require the efforts of staff in IT Branch, Office of Documents and Publication Distribution (ODPD), UI and DI Branch. Every SCDB environment (development, test, production parallel, conversion, training, and production) would have to be restructured and tested separately. During this time, no UI, DI, or BAS programming changes could be released to production.

One-time in-house labor costs alone of this alternative would be approximately $23 million. Vendor costs would be $38 million. With the addition of hardware, software, other related costs, EDD would incur approximately $75 million in one-time costs.   The alternative analysis clearly showed that while this alternative is technologically viable, the costs associated with it are of an order of magnitude greater than the other alternatives. The primary reason for the greater cost overhead is because the SCDB co-mingles the automation requirements of three of EDD's Branches—Unemployment Insurance, Disability Insurance, and Tax Branch—so that it is impossible to upgrade one component of the SCDB system alone. The effort would require a complete rework of all three systems.

Since the scope of this FSR analysis did not take into account UI and Tax Branch baseline costs, it was impossible to determine if this approach is economically viable. Essentially, the

---

[13] COCOMO II Reference Manual, Model Manual, Model Overview, USC, 1999 (http://sunset.usc.edu/COCOMOII/cocomo.html)

vast cost of the project and the lack of organizational will and resources to implement this alternative are prohibitive.

It is also anticipated that IBM's DB2 RDBMS would require more mainframe storage and CPU services than the current IDMS application. According to IBM, most mainframe DB2 implementations increase CPY cycle costs by 50 percent or more. Thus, data center costs would rise accordingly with this solution.

6.0 PROJECT MANAGEMENT PLAN

The EDD recognizes the importance of using industry best practices for project management. This section describes how this project will be managed. It is organized into the following subsections:

6.1   Project Manager Qualifications

6.2   Project Management Methodology

6.3   Project Organization

6.4   Project Priorities

6.5   Project Plan

6.6   Project Monitoring

6.7   Project Quality

6.8   Change Management

6.9   Authorization Required

6.1 Project Manager Qualifications

The Project Manager for this project has not been assigned. The EDD assigns a highly qualified project manager with experience in projects similar to DIAP3. The Project Manager will possess the ability to apply the knowledge, skills, tools, and techniques necessary to successfully complete this project. He/she must possess the following knowledge, education, and experience:

- Minimum of 10 years of experience managing large and complex technology projects in the government sector
- Experience managing Web application development projects
- Undergraduate degree or equivalent experience
- Knowledge of EDD's project management methodology

6.2 Project Management Methodology

This project will use EDD's documented and structured IT Project Management Methodology (IT PMM). The framework is based on the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK®) and is compatible with the Statewide Information Management Manual (SIMM), Section 200. The IT PMM provides standard methods and guidelines to ensure that projects are conducted in a disciplined, well-managed, and consistent manner. It promotes the delivery of quality products that meet the customer's needs and results in project completion on time and within budget.

6.3 Project Organization

The proposed solution requires the addition of new EDD IT staff, plus assistance from consultants to either augment State staff or provide skills State staff do not currently possess. Costs for the proposed resource requirements are detailed in Section 8.0 Economic Analysis Worksheets (EAWS).

Figure 6-1. Organization Chart
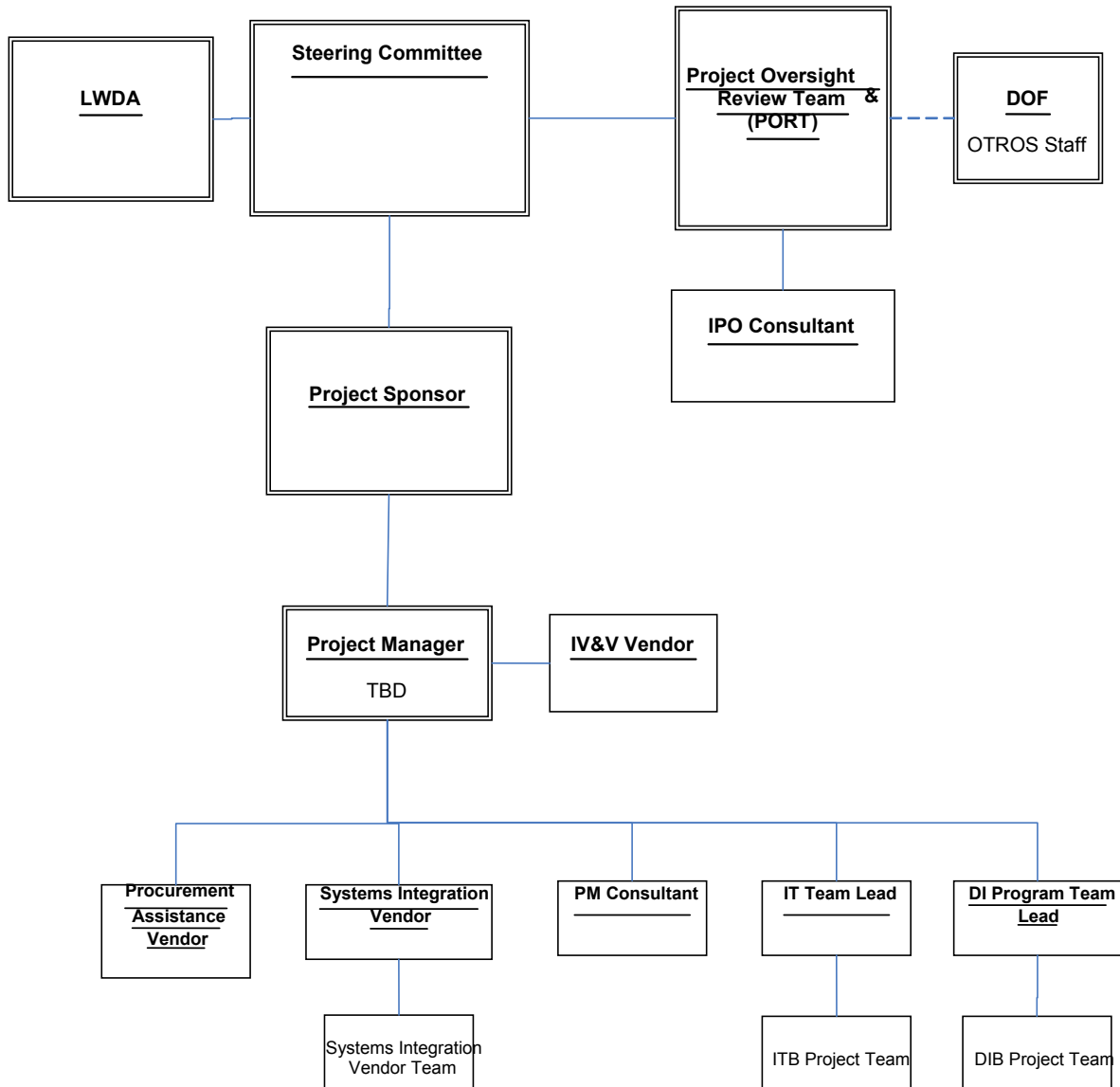
6.4 Project Priorities

Table 6-1. Trade-Off Matrix

	Resources	Schedule	Scope
NOT FLEXIBLE (Cannot change)			X
MOST FLEXIBLE (Could be changed)		X	
FLEXIBLE (Can Be Changed)	X		

- The project **resources** are **flexible.** This means that DI can add additional resources (via contract vehicles) or maximize the use of existing resources by using standardized processes.

- The project **schedule** is classified as **most flexible.** This means that a change in schedule could be acceptable if necessary to preserve scope.

- The project **scope** is **not flexible.** This means that scope cannot change if the current project objectives are to be met. These objectives will be met via implementation of a series of technological initiatives that allows the DIB to further secure, automate, and simplify its numerous manual processes. It implements a solution that complies with the directions and schedules set forth in federal and state HIPAA directives. Those directions emphasize improving the services to DI customers and families, streamlining DI casework, and being a good business partner to those HIPPA covered entities it works with by protecting their information in compliance with HIPAA directives.

6.5 Project Plan

6.5.1 Project Scope

The DI Automation Project, Phase 3 will implement a secure electronic communications and information processing environment by using technologies that will allow DIB to transact business in a HIPAA-compliant manner. The project includes adopting HIPAA guidelines and practices to accomplish further simplification and automation of DIB's numerous manual work processes. The project does not intend to replace the existing SCDB data repository or systems. The project does not intend to make it mandatory for all claims to be submitted electronically.

6.5.2 Project Assumptions

Table 6-2 sets forth the assumptions on which the project is based, the external events upon which the project is dependent, and the constraints under which the project is to be conducted.

Table 6-2. Assumptions, Dependencies, and Constraints

Assumptions
DIB will support HIPAA-covered medical providers in meeting their federal HIPAA mandates.
The proposed solution will meet applicable HIPAA privacy, security, transaction and code set, and administrative simplification requirements.
DIB will utilize existing EDD infrastructure where appropriate.
The project will adhere to a schedule.
Reviewers will provide timely feedback on all deliverables.
Proactive risk, issue, and change management strategies will be employed.
DIB's existing manual processes cannot impede the data flows from and to electronic partners.
Dependencies
EDD resources are available and will be allocated to this effort.
Supporting contracts and procurements will complete on schedule.
A Budget Change Proposal will be required to gain spending approval.
Constraints
The project outcome must comply with EDD's enterprise architecture, standards, and policy.

6.5.3 Project Phasing

The following table depicts the phases anticipated for this project.

Table 6-3. DIAP3 Phases

Project Phase	Phase Deliverables
Phase 1 SI Procurement and Contracting	Award procurement assistance (PA) vendor contract Weekly PA vendor status reports Award IPO consultant contract Weekly IPO consultant status reports Award IV& V vendor contract Weekly IV&V status reports RFP for SI vendor SPR for DIAP3 DGS issue Intent to Award SI contract Award systems integrator contract Award PM consultant contract
Phase 2 Project Start-up and Management	Project Work Plan and Schedule Project Management Plan with Project Charter Weekly IV&V vendor status reports Weekly SI vendor status reports Weekly IPO consultant status reports Weekly PM vendor status reports
Phase 3 Design Solution	Analysis sign-off Design sign-off
Phase 4 Develop and Test Solution	.Net applications sign-off Security sign-off Electronic interface sign-off Intelligent forms sign-off Integration sign-off Complete system test sign-off Scanning/OCR sign-off BPR sign-off
Phase 5 Deploy Solution	Training complete Implementation sign-off Support sign-off
Phase 5 PIER	Approve PIER

6.5.4 Roles and Responsibilities

Table 6-4 lists the project team roles and responsibilities of DIAP3.

Table 6-4. Project Roles and Responsibilities

Role	Responsibility
Steering Committee	Provide EDD leadership and support for project. Provide executive oversight for project. Allocate resources. Interpret federal and state level statutes and executive orders and determine impact on project. Direct policy and procedure changes when needed. Provide final decision making on decisions that could not or should not be made at lower levels. Resolve critical issues which could not or should not be resolved at lower levels. Ensure consistency with EDD Strategic Plan and IT strategies and policies. Ensure consistency with other IT projects and non-IT activities in EDD. Approves all adjustments to project schedule.
Project Sponsor	Serve as an interface to higher-level executive management. Provide necessary funding and resources as appropriate. Champion the project to provide exposure and buy-in from state government and officials. Assign the Project Manager for the project. Work with the assigned project manager to develop the Project Charter. Authorize the project to begin. Review and approve Project Plan. Review and approve all project baselines (scope, schedule and cost). Ensure resources are provided to perform the work. Provide second-level review for issue escalation and change requests. Approve changes to the Project Plan. Review/approve changes in contract commitments. Negotiate with resource managers for resources (staff and/or funding). Communicate information on any changes to project resources. Monitor customer satisfaction with project performance. Secure project funding. Provide staff resources. Approve project baselines and changes to baselines. Assemble and maintain a steering committee with adequate representation of stakeholders from within ITB, other Branches, and entities outside of EDD. Attend and participate, as needed, at Project Status Reviews and steering meetings. Help resolve escalated issues and change requests. Provide representatives to participate in lessons learned sessions. Sign off on Formal Acceptance Form for deliverables and the project itself. Accept/reject the deliverable(s) using the Formal Acceptance Form.

Role	Responsibility
Project Oversight and Review Team (PORT)	Reviews all aspects of development effort to ensure it complies with EDD's project management policies and procedures.
Department of Finance (DOF) – Office of Technology Review, Oversight, and Security (OTROS)	Review IT proposals and ensures IT expenditures represent a prudent investment of resources while meeting the state's business needs. Recommend funding and/or expenditure authority for IT projects, commensurate with the substantiated needs, and any necessary fiscal controls to the Finance Program Budget Manager responsible for a department's budget. Assist Finance to ensure approved IT expenditures are in alignment with statewide IT policies and strategies. Review project status. Advise on resolution of serious project issues. Implement an effective system of independent graduated oversight for all IT projects. Establish statewide standards for project management and oversight. Assess current department/Agency IT project management and oversight practices.
Labor Workforce Development Agency (LWDA)	High level review of project to ensure Agency goals are met.
Project Manager	Work with the Project Sponsor to develop the Project Charter. Ensure that the Project Charter has been approved, and management, customers and contractors have agreed upon the project scope, schedule, quality and resources. Meet and communicate with key stakeholders on a regular basis. Develop a detailed Project Plan with the assistance of the project team to reflect project needs. Incorporate within the Project Plan appropriate reviews and go/no go checkpoints. Ensure that the Project Plan is approved. Ensure that all project baselines are approved. Ensure that stakeholders agree to project commitments. Establish and maintain a Project File containing all project management artifacts. Provide an electronic location for the Project File, and provide access to all the appropriate parties, including the ITB Project Management Office. Arbitrate and resolve conflicts. Shield the project team from undue pressure from customers and/or management. Plan upfront to manage documents with an eye towards facilitating Audit & Evaluation Division's (A&ED) development of the Post-Implementation Evaluation Report (PIER). A&ED expects to refer to documentation that is responsive to the objectives in the FSR and other issues relevant to a PIER (e.g., lessons learned, cost information). Manage day-to-day tasks and provide direction to team members performing work on the project.

Role	Responsibility
	Apply any pertinent lessons learned from previous projects.
	Ensure that the Project Plan is updated and signed off as needed.
	Provide input into new product requirements for the services and/or products that were not planned for in the Planning process group.
	Ensure that the vendors meet the contractual agreements specified within their contracts.
	Track, review and analyze the performance of contractors on a project.
	Administer and oversee the contract as the basis for any changes that need to be made during the life of the contract.
	Manage solicitation and source selection processes and administer contracts as specified by internal EDD contracting policies and procedures.
	Interpret and execute the terms and provisions of the prime contract.
	Integrate all contract activities that involve production management quality control and other contract management functions.
	Act as the focal point with the other contracting party.
	Exercise the functions of subcontract management.
	Price and negotiate subcontracts and contract changes.
	Act as the focal point for conflicts arising under the contract.
	Develop and maintain contract file documentation.
	Ensure adequate project logistics support for vendors.
	Certify invoices for payment.
	Document project work.
	Define, escalate and resolve issues.
	Build team capacity.
	Empower teams.
	Train teams on soft skills
	Ensure training on technical aspects of project, as needed.
	Build in rewards for the project team.
	Provide needed information to project stakeholders as specified in the Communication Management Plan.
	Evaluate overall project performance on a regular basis.
	Make changes to budgets and schedules as approved.
	Produce performance reports, including status reports, performance measurement and forecasting reports.
	Respond to and/or elevate issues and change requests.
	Develop Special Project Reports (SPRs) as required.
	Participate in the change control board to approve product/project changes.
	Review project risks and establish and implement mitigation and contingency procedures.
	Coordinate formal reviews and audits and participate in informal reviews, as defined in the Quality Management Plan.
	Review and act upon the results of quality reviews.
	Verify that control agency, Department and Branch policies are followed.
	Obtain formal acceptance from the sponsor.
	Develop an action plan for any product that does not pass acceptance test.
	Close out open action items.
	Close out any financial accounts or charge codes.

Role	Responsibility
	Assist purchasing contract administrator(s) in contract closure.
	Obtain customer and management approval of completed product.
	Conduct Lessons Learned sessions and prepare the Lessons Learned Report.
	Sign invoices that the Fiscal Programs Division will process for payment.
	Assist as needed with any post-project delivery audits.
	Archive all project data to the project file in a manner that facilitates the development of an eventual Post-Implementation Evaluation Report (PIER).
	Celebrate success with stakeholders and the project team.
IT Team Lead **Program Team Lead**	Assemble information to help the Project Manager prepare the Project Charter.
	May also complete any ancillary Project Initiation materials.
	Coordinate work of the ITB and DIB Project Teams.
	Ensure team responsibilities are met.
ITB Project Team **DIB Project Team**	Develop technical approach.
	Assist in development of estimates and schedules.
	Assist in development of quality assurance processes and the Change Management Plan.
	Identify staff training needs.
	Plan assigned portions of the project in detail.
	Integrate individual plans into the overall project plan.
	Execute assigned project tasks.
	Create product and process solutions.
	Perform quality improvement activities.
	Perform quality assurance activities.
	Learn soft skills and technical project aspects, as needed.
	Escalate issues to Project Manager, as needed.
	Request changes to project scope, schedule and/or resources, as needed.
	Provide stakeholders with information specified in the Communication Management Plan.
	Identify problems, plan responses, and implement plans.
	Identify and respond to risks as specified in the risk management plan.
	Participate in change reviews.
	Track the project execution effort and submit status reports.
	Conduct internal and external reviews and walk-throughs.
	Create testing plan and coordinate test activities.
	Coordinate with Quality Assurance, review QA results, and correct any deviations.
	Participate in lessons learned sessions.
	Identify ways to improve project processes.
	Turn over all project-related documentation to the project manager for archiving.
	Archive project metric data.
	Assess project quality process.

Role	Responsibility
Issue and Change Manager	Communicate issue or change ownership to the appropriate EDD issue owner.
	Present issue and change status to the project team and Executive Steering Committee.
	Record all issues and changes in the issue and change log.
	Ensure that all issues and changes have completed issue and change forms and are filed in the appropriate issue and change file.
	Ensure coordination of adding issues and change implementation into the project plan.
Project Administrator	Prepare financial analyses and budget changes.
	Provide general project support – facilities requests, supplies, meeting coordination, etc.
	Receive, log, distribute, and track deliverables through the approval process.
	Gather and maintain project documentation (project library).
	Support project team meetings - scribe, preparation, logistics.
	Ensure time reporting and contractor billing is accurate.
	Maintain distribution lists and system inventories.
	Make travel arrangements as needed.
Information Security Officer	Attend Executive Steering Committee meetings.
	Participate in and oversee all activities regarding information security and confidentiality.
	Provide final approval of all DI/HIPAA security requirements.
	Provide input to project team pertaining to EDD security and confidentiality requirements.
	Participate in and provide guidance to activities regarding information privacy and confidentiality.
	Provide input to requirements related to data privacy and confidentiality.
Project Configuration Manager	Identify configured items (CIs), tracking and reporting on CIs.
	Develop a Project level Configuration Management Plan.
	Manages physical features, functionality, and documentation of hardware and software developed in the DIAP3 Project.
	Plan and implement configuration change management evaluation processes. Monitor configuration changes. Conduct configuration change control meetings. Prepare status reports. Manage backup and archive configuration records.
	Monitor hardware, software, and desktop configuration inventory.
Procurement Assistance Vendor	Responsible for requirements definition.
	Develop RFP for the systems integration vendor.
	Provide information to DIB and ITB to complete Special Project Report (SPR).
Independent Project Oversight (IPO) Consultant	Performs services under the direction of the PORT.
	Provides independent oversight monitoring and reporting services.

Role	Responsibility
Independent Verification and Validation (IV&V) Vendor	Performs services under the direction of the Project Manager.
	Reviews all aspects of the Systems Integration vendor's work.
	Reviews design, development, and implementation efforts to validate compliance with standards.
	Acts as independent reviewer of project.
Systems Integration (SI) Vendor	Reports to the Project Manager.
	Responsible for development of the new components of DIB solution in the .NET environment as well as overall success of the implementation, including integration with imaging technologies, the IVR, and SCDB.
	Ensure successful end-to end processing of DIB claims and all associated functions.
	Deliver an integrated, functional solution to support DIB program within the required time frame.
Project Management (PM) Consultant	Performs services under the direction of the Project Manager.
	Provides project scheduling, tracking, resource allocation, and reporting support.

6.5.5 Project Schedule

Purchasing preparation for the DIAP3 project is in progress and will continue FSR and ITPP approval, preparation of statements of work, and other acquisition documents. The DIB anticipates funding by July 2006 and expects to complete the project by June 2009. Project review of milestones and decisions will occur at key points throughout the project. The project schedule and approach for phases 2, 3, 4, and 5 will be finalized by EDD and the SI vendor based on the selected solution.

Table 6-5. High-Level Project Schedule

WBS	Task Name	Duration	Start	Finish
1	*DIAP3 Phase 1: Procurement and Contracting*	*782 days*	*Mon 7/3/06*	*Tue 6/30/09*
1.1	Procurement Assistance Vendor	305 days	7/3/06	8/31/07
1.1.1	Award PA contract	0 days	7/3/06	7/3/06
1.1.2	PA vendor contract	305 days	7/3/06	8/31/07
1.1.3	Knowledge transfer with IV&V vendor	65 days	6/4/07	8/31/07
1.1.4	PA Weekly Status	301 days	7/3/06	8/27/07
1.2	Independent Project Oversight Consultant	781 days	7/3/06	6/29/09
1.2.1	Award IPO contract	0 days	7/3/06	7/3/06
1.2.2	IPO consultant contract	738 days	7/3/06	4/29/09
1.2.3	IPO Weekly Status	781 days	7/3/06	6/29/09
1.3	IV&V Vendor	782 days	7/3/06	6/30/09
1.3.1	Award IV&V contract	0 days	7/3/06	7/3/06

WBS	Task Name	Duration	Start	Finish
1.3.2	IV&V vendor contract	782 days	7/3/06	6/30/09
1.3.3	Knowledge transfer with PA vendor	65 days	6/4/07	8/31/07
1.3.4	IV&V Weekly Status	781 days	7/3/06	6/29/09
1.4	SI Vendor Procurement	782 days	7/3/06	6/30/09
1.4.1	Prepare RFP	80 days	7/3/06	10/20/06
1.4.2	Assist with acquisition	180 days	10/23/06	6/29/07
1.4.3	Prepare SPR	30 days	3/1/07	4/11/07
1.4.4	Obtain OTROS approval	0 days	6/20/07	6/20/07
1.4.5	DGS issue Intent to Award	0 days	6/22/07	6/22/07
1.4.6	Award SI vendor contract	0 days	7/2/07	7/2/07
1.4.7	SI Vendor Contract	522 days	7/2/07	6/30/09
1.5	PM Consultant	523 days	6/29/07	6/30/09
1.5.1	Award PM contract	0 days	6/29/07	6/29/07
1.5.2	PM vendor contract	522 days	7/2/07	6/30/09
1.5.3	Weekly PM status	516 days	7/9/07	6/29/09
2	DIAP3 Phase 2: Project Start-up and Management	520 days	Mon 7/2/07	Fri 6/26/09
2.1	Planning and Control	520 days	Mon 7/2/07	Fri 6/26/09
2.1.1	Finalize project work plan and schedule	8 days	Mon 7/2/07	Wed 7/11/07
2.1.2	Project work plan and schedule	0 days	Wed 7/11/07	Wed 7/11/07
2.1.3	Finalize project management plan with charter	12 days	Mon 7/2/07	Tue 7/17/07
2.1.4	PMP and Project Charter	0 days	Tue 7/17/07	Tue 7/17/07
2.1.5	Weekly SI status	516 days	Fri 7/6/07	Fri 6/26/09
2.1.6	Monthly steering committee review	479 days	Wed 8/15/07	Mon 6/15/09
3	DIAP3 Phase 3: Design Solution	98 days	Wed 7/18/07	Fri 11/30/07
3.1	Analysis	30 days	Wed 7/18/07	Tue 8/28/07
3.1.1	Technical analysis	16 days	Wed 7/18/07	Wed 8/8/07
3.1.1.1	Define current systems	3 days	Wed 7/18/07	Fri 7/20/07
3.1.1.2	Define current infrastructure	3 days	Mon 7/23/07	Wed 7/25/07
3.1.1.3	Define interfaces	5 days	Thu 7/26/07	Wed 8/1/07
3.1.1.4	Define current security	5 days	Thu 8/2/07	Wed 8/8/07
3.1.2	Functional analysis	30 days	Wed 7/18/07	Tue 8/28/07
3.1.2.1	Define current business processes	30 days	Wed 7/18/07	Tue 8/28/07
3.1.3	Analysis sign-off	0 days	Tue 8/28/07	Tue 8/28/07
3.2	Design	68 days	Wed 8/29/07	Fri 11/30/07
3.2.1	Technical design	68 days	Wed 8/29/07	Fri 11/30/07
3.2.1.1	Design applications	60 days	Wed 8/29/07	Tue 11/20/07

WBS	Task Name	Duration	Start	Finish
3.2.1.2	Design infrastructure changes (if any)	5 days	Wed 11/21/07	Tue 11/27/07
3.2.1.3	Design interfaces	15 days	Mon 11/5/07	Fri 11/23/07
3.2.1.4	Design security	15 days	Mon 11/12/07	Fri 11/30/07
3.2.2	Functional design	30 days	Wed 8/29/07	Tue 10/9/07
3.2.2.1	Design new business processes	30 days	Wed 8/29/07	Tue 10/9/07
3.2.3	Design sign-off	0 days	Fri 11/30/07	Fri 11/30/07
4	*DIAP3 Phase 4: Develop and Test Solution*	*338 days*	*Wed 8/29/07*	*Fri 12/12/08*
4.1	Establish technical test environment	30 days	Wed 8/29/07	Tue 10/9/07
4.2	Track 1-.Net Applications	200 days	Mon 12/3/07	Fri 9/5/08
4.2.1	Develop/test .Net applications	200 days	Mon 12/3/07	Fri 9/5/08
4.2.2	Track 1 sign-off	0 days	Fri 9/5/08	Fri 9/5/08
4.3	Track 2-Security	130 days	Mon 3/17/08	Fri 9/12/08
4.3.1	Develop/test security	130 days	Mon 3/17/08	Fri 9/12/08
4.3.2	Track 2 sign-off	0 days	Fri 9/12/08	Fri 9/12/08
4.4	Track 3-Electronic Interface	86 days	Tue 5/20/08	Tue 9/16/08
4.4.1	Develop/test direct e-interface intake	86 days	Tue 5/20/08	Tue 9/16/08
4.4.2	Track 3 sign-off	0 days	Tue 9/16/08	Tue 9/16/08
4.5	Track 4-Intelligent Forms	42 days	Wed 7/23/08	Thu 9/18/08
4.5.1	Develop/test intelligent forms intake	42 days	Wed 7/23/08	Thu 9/18/08
4.5.2	Track 4 sign-off	0 days	Thu 9/18/08	Thu 9/18/08
4.6	Track 5-Integration	105 days	Tue 4/22/08	Mon 9/15/08
4.6.1	Develop/test interfaces	100 days	Tue 4/22/08	Mon 9/8/08
4.6.2	Develop/test integration	80 days	Tue 5/27/08	Mon 9/15/08
4.6.3	Track 5 sign-off	0 days	Mon 9/15/08	Mon 9/15/08
4.7	Track 6-Complete System Test	10 days	Fri 9/19/08	Thu 10/2/08
4.7.1	Test all solution components	10 days	Fri 9/19/08	Thu 10/2/08
4.7.2	System test sign-off	0 days	Thu 10/2/08	Thu 10/2/08
4.8	Track 7-Scanning/OCR	30 days	Fri 10/3/08	Thu 11/13/08
4.8.1	Develop/test scanning/OCR	30 days	Fri 10/3/08	Thu 11/13/08
4.8.2	Track 7 sign-off	0 days	Thu 11/13/08	Thu 11/13/08
4.9	Track 8-Business Process Reengineering	70 days	Mon 9/8/08	Fri 12/12/08
4.9.1	Develop new/reengineer process	70 days	Mon 9/8/08	Fri 12/12/08
4.9.2	Track 8 sign-off	0 days	Fri 12/12/08	Fri 12/12/08
5	*DIAP3 Phase 5: Deploy Solution*	*142 days*	*Mon 12/15/08*	*Tue 6/30/09*
5.1	Implement Business Processes	30 days	Mon 12/15/08	Fri 1/23/09
5.1.1	Final BPR activities	30 days	Mon 12/15/08	Fri 1/23/09

WBS	Task Name	Duration	Start	Finish
5.2	Change Management	80 days	Mon 12/15/08	Fri 4/3/09
5.2.1	Marketing, communications	80 days	Mon 12/15/08	Fri 4/3/09
5.3	Training	65 days	Mon 1/5/09	Fri 4/3/09
5.3.1	Technical	20 days	Mon 1/5/09	Fri 1/30/09
5.3.2	Mainframe	15 days	Mon 1/12/09	Fri 1/30/09
5.3.3	User	45 days	Mon 2/2/09	Fri 4/3/09
5.3.4	Stakeholder	15 days	Mon 3/16/09	Fri 4/3/09
5.4	Implementation	85 days	Mon 2/2/09	Fri 5/29/09
5.4.1	Headquarters	20 days	Mon 2/2/09	Fri 2/27/09
5.4.2	Statewide	75 days	Mon 2/16/09	Fri 5/29/09
5.4.3	Implementation sign-off	0 days	Fri 5/29/09	Fri 5/29/09
5.5	On-site Support	22 days	Mon 6/1/09	Tue 6/30/09
5.5.1	Support/tuning	22 days	Mon 6/1/09	Tue 6/30/09
5.5.2	Support sign-off	0 days	Tue 6/30/09	Tue 6/30/09

The following Gantt chart shows the timeline for the project.

Figure 6-2. High-level DIAP3 Timeline

6.6 Project Monitoring

The EDD IT PMM project reporting and monitoring process will be used for this project. Status reports will act as a vehicle to oversee that the project's scope; budget, and time are within acceptable guidelines as set forth in the FSR. In addition, EDD will work with project management and IV&V vendors to incorporate their knowledge, expertise, and skills in comparable projects to provide additional recommendations regarding best practices.

6.7 Project Quality

Quality assurance will be monitored using EDD's IT PMM quality control procedures. Procedures include separation of duties, acceptance testing, version control tools, requirements traceability matrix, and customer walk-through. The project management vendor will assist in the development of quality standards and their implementation for this project; the IV&V vendor will validate the project's adherence to the plan and evaluate products to ensure they meet

quality standards. The DIB, ITB, and the vendors will collaborate to ensure quality of design, development, and testing of the new system.

6.8 Change Management

The project team will utilize the existing change management processes as defined within the IT PMM framework. In addition, the Sponsor must approve significant changes to project baselines (cost, schedule, scope, and quality). During development, the project team will use EDD's configuration management processes.

6.9 Authorization Required

No special authorization such as federal approval or legislative review is required.

7.0 RISK MANAGEMENT PLAN

The project's Risk Management Plan will document the processes and procedures used to identify risks associated with the project and how they will be managed. The project will follow the risk management processes identified by EDD's ITB Project Management Office and the State Information Management Manual (SIMM).

7.1 Risk Management Worksheet

Risk #	Risk Category	Risk Event Title	Risk Event Desc.	Origin-ator	Origin. Date	Impact (H-M-L)	Prob-ability (H-M-L)	Exposure (calc'd)	Time Frame (S-M-L)	Sever-ity (calc'd)	Risk Response Strategy	Mitigation / Prevention Plan	Conting-ency Plan	Risk Owner	Risk Tracking	Comments	Status
1	Procure-ment		Procurement process takes longer than expected	Project Team	5/20/04	H	L	M	L	L	Avoidance	Seek assistance from control agencies Expedite decision making Adjust schedule		Project Sponsor		EDD staff involved in implementing PFL has a sense of urgency and understands the time constraints	
2	Procure-ment		Vendor protests bid award	Project Team	5/20/04	M	L	L	M	L	Mitigation	Seek assistance from control agencies Expedite decision making Adjust schedule		Project Sponsor			
3	Develop-ment Env.		Vendor Image Processing environment (imaging) may not be available when needed	Project Team	5/20/04	H	H	H	M	H	Mitigation	Develop clear specifications upon which to develop RFP to subcontract this work out	Imaging component to be contracted out	Project Sponsor			
4	Develop-ment Env.		Vendor Image Processing environment (imaging) may not have enough capacity	Project Team	5/20/04	H	H	H	M	H	Mitigation	Develop clear specifications upon which to develop RFP to subcontract this work out	Imaging component to be contracted out	Project Sponsor			

Risk #	Risk Category	Risk Event Title	Risk Event Desc.	Origin-ator	Origin. Date	Impact (H-M-L)	Prob-ability (H-M-L)	Exposure (calc'd)	Time Frame (S-M-L)	Sever-ity (calc'd)	Risk Response Strategy	Mitigation / Prevention Plan	Conting-ency Plan	Risk Owner	Risk Tracking	Comments	Status
5	Contractor Perf.		General contractor fails to meet milestones as expected	Project Team	5/20/04	H	L	M	M	M	Mitigation	Define liquidated damage strategy Engage IV&V	Enact holdbacks in contract payments, only contract with vendors with solid track record The DI Automation Project Phase 3 will be managed by experienced project managers and will incorporate EDD risk and project management standards. Will utilize PM support and IV&V vendors to mitigate risk	Project Sponsor			
6	Contractor Perf.		Contractor's deliverables do not meet requirements	Project Team	5/20/04	M	L	L	M	L	Mitigation	Engage IV&V Engage integration vendor Requirements and deliverables will be closely monitored to ensure the quality of the work. IV&V and Project Management Support vendors will be contracted to ensure industry	Enact holdbacks in contract payments, only contract with vendors with solid track record The DI Automation Project Phase 3 will be managed by experienced	Project Sponsor		It is expected that the RFP process will closely scrutinize the quality of work the selected vendor has delivered in previous engagements	

Risk #	Risk Category	Risk Event Title	Risk Event Desc.	Origin-ator	Origin. Date	Impact (H-M-L)	Prob-ability (H-M-L)	Exposure (calc'd)	Time Frame (S-M-L)	Sever-ity (calc'd)	Risk Response Strategy	Mitigation / Prevention Plan	Conting-ency Plan	Risk Owner	Risk Tracking	Comments	Status
												best practices are applied	project managers and will incorporate EDD risk and project management standards. Will utilize PM support and IV&V vendor.				
7	Contractor Perf.		Timeliness	Project Team	5/20/04	M	M	M	M	M	Mitigation	Establish pre-delivery inspection points	Adjust scope of work or add resources to meet quality requirements	Project Sponsor			
8	Contractor Perf.		Lack of participation of external stakeholders	Project Team	5/20/04	L	L	L	M	L	Mitigation	Marketing to external stakeholders		Project Sponsor			
9	Personnel		Unplanned turnover of State key personnel	Project Team	5/20/04	L	L	L	M	L	Acceptance/ Contingency	Cross train staff. Well defined and phased project scope and leverage existing EDD processes and technology solutions. Use of contracted resources to augment EDD resources.	Outsource	Project Sponsor			

Risk #	Risk Category	Risk Event Title	Risk Event Desc.	Origin-ator	Origin. Date	Impact (H-M-L)	Prob-ability (H-M-L)	Exposure (calc'd)	Time Frame (S-M-L)	Sever-ity (calc'd)	Risk Response Strategy	Mitigation / Prevention Plan	Conting-ency Plan	Risk Owner	Risk Tracking	Comments	Status
10	Personnel		ITB resources are unavailable at time needed.	Project Team	5/20/04	H	M	H	M	H	Mitigation	Inter-agency agreements Clearly defined resource requirements perform skills assessment to better manage available resources	Additional resources will be assigned to support the PFL solution. Any skill set gaps will be identified and training provided	Project Sponsor			
11	System Security		Inability to provide adequate HIPAA level security may cause non participation by external stakeholders	Project Team	5/20/04	M	L	L	M	L	Mitigation	DI funds and puts in place telecommunicati ons and operational security	Outsource	Project Sponsor			
12	Design & Implem.		Vendor design takes longer than expected	EPC	5/25/04	H	L	M	M	M	Mitigation	Ensure business requirements are clearly stated in bid awarded		Project Sponsor			
13	Design & Implem.		High error rate in the scanning of claim forms	EPC	5/25/04	M	L	L	M	L	Mitigation	Manual key from image and key from paper processes are in place		Project Sponsor			

7.1.1 Assessment

The Risk Management Worksheet identifies the potential sources of risk associated with this project. The risks identified on the worksheet will be re-evaluated on a monthly basis throughout the project. In addition, the project manager will include all identified risks in the detailed project plan using EDD's standard project management planning tools. This plan will encompass the entire structure of the project and its deliverables, providing a comprehensive framework for assessing each aspect of the project for potential risk.

7.1.2 Risk Identification

Staff identified potential internal and external risks. The following tools were used to aid in the identification of risks:

- SIMM categories and examples of risk

- Work breakdown structure

- Historical information

- Project team brainstorming

- Interviews with stakeholders

The characteristics of each identified risk are captured on the Risk Management Worksheet.

7.1.3 Risk Analysis and Quantification

The risk session facilitated the evaluation of particular identified risks to assess the range of possible project outcomes. Each identified risk was fully discussed and understood during the decision-making process. The risk analysis and quantification process led to the production of the Risk Management Worksheet and documented the sources of risk and risk events that the project team decided to accept.

7.1.4 Risk Prioritization

During the risk session, the identified risks were ranked and the potential impact or consequence to mission and business objectives were considered.

7.1.4 Risk Response

The risk session identified the factors of schedule, resources, and stakeholder risk tolerances. The project manager is responsible for responding to risk areas that include avoidance, acceptance, mitigation, sharing, and project oversight.

7.1.5 Risk Avoidance

The risk session produced preventive and contingency measures to eliminate the risk or lessen the risk impact to the project.

7.1.6 Risk Acceptance

Each member of the risk session agreed to accept each risk event and the consequences.

7.1.7 Risk Mitigation

Risk mitigation measures were identified during the session.

7.1.8 Risk Sharing

The project manager will be responsible to delegate and manage those activities that have a risk factor associated.

7.2 Risk Tracking and Control

7.2.1 Risk Tracking

The project manager will be responsible for establishing and maintaining risk status information, defining action plans, and taking corrective action when appropriate. Risks will be formally reviewed on a monthly basis, or more frequently if required. Risk escalation requirements as defined in the SIMM will be followed. The Risk Management Plan will be used in order to respond to risk events throughout the life of the project.

7.2.2 Risk Control

The project manager will oversee the execution of the Risk Management Plan in order to respond to risk events before they become serious problems. The project manager will also ensure that risk procedures are documents and executed according to the plan. As anticipated risk events occur or fail to occur, and as actual risk events are evaluated and resolved, the project manager will routinely update the Risk Management Plan.

8.0 ECONOMIC ANALYSIS WORKSHEETS

The worksheets included in this section analyze the costs associated with the two alternatives for implementing information systems to support the DI Automation Project Phase 3.

EXISTING SYSTEM/BASELINE COST WORKSHEET

Department: EDD - Disability Insurance Branch   All costs to be shown in whole (unrounded) dollars.   Date Prepared: 06/06/05

Project: DI Automation Project Phase 3

	FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		FY 2010/11		FY 2011/12		TOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
Continuing Information Technology Costs														
Staff (salaries & benefits)	52.4	4,877,659	52.4	4,877,659	52.4	4,877,659	52.4	4,877,659	52.4	4,877,659	52.4	4,877,659	**314.5**	29,265,955
Hardware Lease/Maintenance		33,048		33,048		33,048		33,048		33,048		33,048		198,288
Software Maintenance/Licenses		102,227		102,227		102,227		102,227		102,227		102,227		613,362
Contract Services		5,000		5,000		5,000		5,000		5,000		5,000		30,000
Data Center Services		2,323,465		2,323,465		2,323,465		2,323,465		2,323,465		2,323,465		13,940,791
Agency Facilities		0		0		0		0		0		0		0
Other		2,419,692		2,419,692		2,419,692		2,419,692		2,419,692		2,419,692		14,518,152
Total IT Costs	**52.4**	**9,761,091**	**52.4**	**9,761,091**	**52.4**	**9,761,091**	**52.4**	**9,761,091**	**52.4**	**9,761,091**	**52.4**	**9,761,091**	**314.5**	**58,566,548**
Continuing Program Costs:														
Staff	853.3	44,564,805	864.9	45,171,030	876.7	45,786,348	888.6	46,410,896	900.8	47,044,893	913.1	47,688,342	**5297.3**	**276,666,316**
Other		0		0		0		0		0		0		**0**
Total Program Costs	**853.3**	**44,564,805**	**864.9**	**45,171,030**	**876.7**	**45,786,348**	**888.6**	**46,410,896**	**900.8**	**47,044,893**	**913.1**	**47,688,342**	**5297.3**	**276,666,316**
TOTAL EXISTING SYSTEM COST	**905.7**	**54,325,896**	**917.3**	**54,932,121**	**929.1**	**55,547,440**	**941.0**	**56,171,988**	**953.2**	**56,805,985**	**965.5**	**57,449,434**	**5611.8**	**335,232,864**

EDD Employment Development Department State of California

PROPOSED ALTERNATIVE: Web-Based Initiative

Date Prepared: 06/06/05

Department: EDD - Disability Insurance Branch   All Costs Should be shown in whole (unrounded) dollars.

Project: DI Automation Project Phase 3

	FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		FY 2010/11		FY 2011/12		TOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
One-Time IT Project Costs														
Staff (Salaries & Benefits)	6.3	593,198	24.8	2,270,442	28.6	2,591,544	0.0	0	0.0	0	0.0	0	59.7	5,455,184
Hardware Purchase		12,390		694,235		188,260	0.0	0	0.0	0	0.0	0		894,885
Software Purchase/License		0		1,667,680		0	0.0	0	0.0	0	0.0	0		1,667,680
Telecommunications		0		60,000		7,000	0.0	0	0.0	0	0.0	0		67,000
Contract Services														0
Software Customization		0		4,107,500		5,200,000	0.0	0	0.0	0	0.0	0		9,307,500
Project Management		0		218,750		218,750	0.0	0	0.0	0	0.0	0		437,500
Project Oversight		100,000		120,000		120,000	0.0	0	0.0	0	0.0	0		340,000
IV&V Services		500,000		1,000,000		1,000,000	0.0	0	0.0	0	0.0	0		2,500,000
Other Contract Services		400,000		225,000		1,525,000	0.0	0	0.0	0	0.0	0		2,150,000
TOTAL Contract Services		1,000,000		5,671,250		8,063,750	0.0	0	0.0	0	0.0	0		14,735,000
Data Center Services		0		0		2,700	0.0	0	0.0	0	0.0	0		2,700
Agency Facilities		0		0		0	0.0	0	0.0	0	0.0	0		0
Other		153,191		592,505		1,163,449	0.0	0	0.0	0	0.0	0		1,909,145
Total One-time IT Costs	6.3	1,758,779	24.8	10,956,112	28.6	12,016,703	0.0	0	0.0	0	0.0	0	59.7	24,731,595
Continuing IT Project Costs														
Staff (Salaries & Benefits)	0.0	0	0.0	0	0.0	0	12.4	1,164,421	12.4	1,164,421	12.4	1,164,421	37.3	3,493,264
Hardware Lease/Maintenance		0		0		111,000		147,000		147,000		147,000		552,000
Software Maintenance/Licenses		0		0		292,136		284,112		284,112		284,112		1,144,472
Telecommunications				0		12,000		12,000		12,000		12,000		48,000
Contract Services		0		0		0		1,453,516		1,197,476		1,139,476		3,790,468
Data Center Services		0		0		195,408		195,408		195,408		195,408		781,632
Agency Facilities		0		0		0		0		0		0		0
Other		0		0		5,000		294,655		294,655		294,655		888,966
Total Continuing IT Costs	0.0	0	0.0	0	0.0	615,544	12.4	3,551,113	12.4	3,295,073	12.4	3,237,073	37.3	10,698,802
Total Project Costs	6.3	1,758,779	24.8	10,956,112	28.6	12,632,247	12.4	3,551,113	12.4	3,295,073	12.4	3,237,073	97.0	35,430,397
Continuing Existing Costs														
Information Technology Staff	52.4	4,877,659	52.4	4,877,659	52.4	4,877,659	52.4	4,877,659	52.4	4,877,659	52.4	4,877,659	314.5	29,265,954
Other IT Costs		4,883,432		4,883,432		4,883,432		4,883,432		4,883,432		4,883,432		29,300,593
Total Continuing Existing IT Costs	52.4	9,761,091	52.4	9,761,091	52.4	9,761,091	52.4	9,761,091	52.4	9,761,091	52.4	9,761,091	314.5	58,566,547
Program Staff	853.3	44,564,805	864.9	45,171,030	876.7	45,786,348	808.5	42,226,338	728.8	38,064,289	668.4	34,908,673	4800.5	250,721,483
Other Program Costs		0		0		0		0		0		0		0
Total Continuing Existing Program Costs	853.3	44,564,805	864.9	45,171,030	876.7	45,786,348	808.5	42,226,338	728.8	38,064,289	668.4	34,908,673	4800.5	250,721,483
Total Continuing Existing Costs	905.7	54,325,896	917.3	54,932,121	929.1	55,547,440	860.9	51,987,429	781.2	47,825,380	720.8	44,669,764	5115.0	309,288,031
TOTAL ALTERNATIVE COSTS	912.0	56,084,676	942.1	65,888,234	957.7	68,179,687	873.3	55,538,542	793.7	51,120,453	733.2	47,906,837	5212.0	344,718,427
INCREASED REVENUES		0		0		0		0		0		0		0

ALTERNATIVE #1:   **Mainframe-based Automation Initiative**

Date Prepared: 06/06/05

Department: EDD - Disability Insurance Branch   All Costs Should be shown in whole (unrounded) dollars.

Project: DI Automation Project Phase 3

	FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		FY 2010/11		FY 2011/12		TOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
One-Time IT Project Costs														
Staff (Salaries & Benefits)	46.6	4,166,006	96.4	8,647,225	113.5	10,163,742	0.0	0	0.0	0	0.0	0	256.5	22,976,973
Hardware Purchase		637,380		425,745		0		0		0		0		1,063,125
Software Purchase/License		3,819,500		1,249,680		0		0		0		0		5,069,180
Telecommunications		0		60,000		7,000		0		0		0		67,000
Contract Services														
Software Customization		5,134,030		10,505,560		11,048,060		0		0		0		26,687,650
Project Management		218,750		218,750		218,750		0		0		0		656,250
Project Oversight		96,000		120,000		120,000		0		0		0		336,000
IV&V Services		1,400,000		2,800,000		2,800,000		0		0		0		7,000,000
Other Contract Services		0		1,026,800		1,865,200		0		0		0		2,892,000
TOTAL Contract Services		6,848,780		14,671,110		16,052,010		0		0		0		37,571,900
Data Center Services		0		350,000		2,700		0		0		0		352,700
Agency Facilities		0		0		0		0		0		0		0
Other		1,299,692		2,363,059		3,247,721		0		0		0		6,910,472
Total One-time IT Costs	46.6	16,771,358	96.4	27,766,818	113.5	29,473,173	0.0	0	0.0	0	0.0	0	256.5	74,011,350
Continuing IT Project Costs														
Staff (Salaries & Benefits)	0.0	0	0.0	0	11.4	453,403	22.8	1,434,702	22.8	1,434,702	22.8	1,434,702	79.8	4,757,511
Hardware Lease/Maintenance		-		-		96,000		141,000		141,000		141,000		519,000
Software Maintenance/Licenses		0		0		250,336		909,242		909,242		909,242		2,978,063
Telecommunications		0		12,000		12,000		12,000		12,000		12,000		60,000
Contract Services		0		0		0		1,253,516		1,197,476		1,139,476		3,590,468
Data Center Services		0		0		545,408		545,408		545,408		545,408		2,181,632
Agency Facilities		0		0		0		0		0		0		0
Other	0.0	0	0.0	0	0.0	238,636	0.0	626,530	0.0	493,062	0.0	493,062		1,851,291
Total Continuing IT Costs	0.0	0	0.0	12,000	11.4	1,595,783	22.8	4,922,399	22.8	4,732,891	22.8	4,674,891	79.8	15,937,965
Total Project Costs	46.6	16,771,358	96.4	27,778,818	124.9	31,068,956	22.8	4,922,399	22.8	4,732,891	22.8	4,674,891	336.3	89,949,314
Continuing Existing Costs														
Information Technology Staff	52.4	4,877,659	52.4	4,877,659	52.4	4,877,659	52.4	4,877,659	52.4	4,877,659	52.4	4,877,659	314.5	29,265,955
Other IT Costs		4,883,432		4,883,432		4,883,432		4,883,432		4,883,432		4,883,432		29,300,592
Total Continuing Existing IT Costs	52.4	9,761,091	52.4	9,761,091	52.4	9,761,091	52.4	9,761,091	52.4	9,761,091	52.4	9,761,091	314.5	58,566,547
Program Staff	853.3	44,564,805	864.9	45,171,030	876.7	45,786,348	808.5	42,226,338	728.8	38,064,289	668.4	34,908,673	4800.5	250,721,483
Other Program Costs		0		0		0		0		0		0		0
Total Continuing Existing Program Costs	853.3	44,564,805	864.9	45,171,030	876.7	45,786,348	808.5	42,226,338	728.8	38,064,289	668.4	34,908,673	4,800.5	250,721,483
Total Continuing Existing Costs	905.7	54,325,896	917.3	54,932,121	929.1	55,547,440	860.9	51,987,429	781.2	47,825,380	720.8	44,669,764	5,115.1	309,288,030
TOTAL ALTERNATIVE COSTS	952.2	71,097,254	1013.7	82,710,940	1054.0	86,616,396	883.7	56,909,828	804.0	52,558,271	743.6	49,344,655	5,451.4	399,237,344
INCREASED REVENUES		0		0		0		0		0		0		0

ECONOMIC ANALYSIS SUMMARY

Date Prepared: 06/06/05

Department: EDD - Disability Insurance Branch All costs to be shown in whole (unrounded) dollars.

Project: DI Automation Project Phase 3

	FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		FY 2010/11		FY 2011/12		TOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
EXISTING SYSTEM														
Total IT Costs	52.4	9,761,091	52.4	9,761,091	52.4	9,761,091	52.4	9,761,091	52.4	9,761,091	52.4	9,761,091	314.5	58,566,548
Total Program Costs	853.3	44,564,805	864.9	45,171,030	876.7	45,786,348	888.6	46,410,896	900.8	47,044,893	913.1	47,688,342	5297.3	276,666,316
Total Existing System Costs	905.7	54,325,896	917.3	54,932,121	929.1	55,547,440	941.0	56,171,988	953.2	56,805,985	965.5	57,449,434	5611.8	335,232,864
PROPOSED ALTERNATIVE							**Web-Based Initiative**							
Total Project Costs	6.3	1,758,779	24.8	10,956,112	28.6	12,632,247	12.4	3,551,113	12.4	3,295,073	12.4	3,237,073	97.0	35,430,397
Total Cont. Exist. Costs	905.7	54,325,896	917.3	54,932,121	929.1	55,547,440	860.9	51,987,429	781.2	47,825,380	720.8	44,669,764	5115.0	309,288,031
Total Alternative Costs	912.0	56,084,676	942.1	65,888,234	957.7	68,179,687	873.3	55,538,542	793.7	51,120,453	733.2	47,906,837	5212.0	344,718,427
COST SAVINGS/AVOIDANCES	(6.3)	(1,758,779)	(24.8)	(10,956,112)	(28.6)	(12,632,247)	67.7	633,446	159.5	5,685,532	232.3	9,542,597	399.8	(9,485,564)
Increased Revenues		0		0		0		0		0		0		0
Net (Cost) or Benefit	(6.3)	(1,758,779)	(24.8)	(10,956,112)	(28.6)	(12,632,247)	67.7	633,446	159.5	5,685,532	232.3	9,542,597	399.8	(9,485,564)
Cum. Net (Cost) or Benefit	(6.3)	(1,758,779)	(31.1)	(12,714,892)	(59.7)	(25,347,139)	8.0	(24,713,693)	167.5	(19,028,161)	399.8	(9,485,564)		
ALTERNATIVE #1							**Mainframe-based Automation Initiative**							
Total Project Costs	46.6	16,771,358	96.4	27,778,818	124.9	31,068,956	22.8	4,922,399	22.8	4,732,891	22.8	4,674,891	336.3	89,949,314
Total Cont. Exist. Costs	905.7	54,325,896	917.3	54,932,121	929.1	55,547,440	860.9	51,987,429	781.2	47,825,380	720.8	44,669,764	5115.1	309,288,030
Total Alternative Costs	952.2	71,097,254	1013.7	82,710,940	1054.0	86,616,396	883.7	56,909,828	804.0	52,558,271	743.6	49,344,655	5451.4	399,237,344
COST SAVINGS/AVOIDANCES	(46.6)	(16,771,358)	(96.4)	(27,778,818)	(124.9)	(31,068,956)	57.3	(737,840)	149.2	4,247,714	221.9	8,104,778	160.5	(64,004,481)
Increased Revenues		0		0		0		0		0		0		0
Net (Cost) or Benefit	(46.6)	(16,771,358)	(96.4)	(27,778,818)	(124.9)	(31,068,956)	57.3	(737,840)	149.2	4,247,714	221.9	8,104,778	160.5	(64,004,481)
Cum. Net (Cost) or Benefit	(46.6)	(16,771,358)	(143.0)	(44,550,176)	(267.9)	(75,619,132)	(210.6)	(76,356,973)	(61.4)	(72,109,259)	160.5	(64,004,481)		

PROJECT FUNDING PLAN

Department: EDD - Disability Insurance Branch   All costs to be shown in whole (unrounded) dollars.   Date Prepared: 06/06/05

Project: DI Automation Project Phase 3

	FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		FY 2010/11		FY 2011/12		TOTALS	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
TOTAL PROJECT COSTS	6.3	1,758,779	24.8	10,956,112	28.6	12,632,247	12.4	3,551,113	12.4	3,295,073	12.4	3,237,073	97.0	35,430,397
RESOURCES TO BE REDIRECTED														
Staff	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	**0.0**	**0.0**
Funds:														
Existing System		0		0		0		0		0		0		**0**
Other Fund Sources		0		0		0		0		0		0		**0**
TOTAL REDIRECTED RESOURCES	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0
ADDITIONAL PROJECT FUNDING NEEDED														
One-Time Project Costs	6.3	1,758,779	24.8	10,956,112	28.6	12,016,703	0.0	0	0.0	0	0.0	0	**60**	**24,731,595**
Continuing Project Costs	0.0	0	0.0	0	0.0	615,544	12.4	3,551,113	12.4	3,295,073	12.4	3,237,073	**37**	**10,698,802**
TOTAL ADDITIONAL PROJECT FUNDS NEEDED BY FISCAL YEAR	6.3	1,758,779	24.8	10,956,112	28.6	12,632,247	12.4	3,551,113	12.4	3,295,073	12.4	3,237,073	97	35,430,397
TOTAL PROJECT FUNDING	6.3	1,758,779	24.8	10,956,112	28.6	12,632,247	12.4	3,551,113	12.4	3,295,073	12.4	3,237,073	97	35,430,397
Difference: Funding - Costs	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0.0	0	0	0
Total Estimated Cost Savings	0.0	0	0	0	0	0	67.7	3,535,803	159.5	8,331,849	232.3	12,130,914	**459**	**23,998,566**

ADJUSTMENTS, SAVINGS AND REVENUES
(DOF Use Only)

Department: EDD - Disability Insurance Bran

Project: DI Automation Project Phase 3

Date Prepared: 06/06/05

Annual Project Adjustments	FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		FY 2010/11		FY 2011/12		Net Adjustments	
	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts	PYs	Amts
One-time Costs														
Previous Year's Baseline	0.0	0	6.3	1,758,779	24.8	10,956,112	28.6	12,016,703	0.0	0	0.0	0		
(A) Annual Augmentation /(Reduction)	**6.3**	**1,758,779**	**18.5**	**9,197,333**	**3.8**	**1,060,591**	**(28.6)**	**(12,016,703)**	**0.0**	**0**	**0.0**	**0**		
(B) Total One-Time Budget Actions	6.3	1,758,779	24.8	10,956,112	28.6	12,016,703	0.0	0	0.0	0	0.0	0	**59.7**	**24,731,595**
Continuing Costs											0.0		59.7	
Previous Year's Baseline	0.0	0	0.0	0	0.0	0	0.0	615,544	12.4	3,551,113	12.4	3,295,073		
(C) Annual Augmentation /(Reduction)	**0.0**	**0**	**0.0**	**0**	**0.0**	**615,544**	**12.4**	**2,935,569**	**0.0**	**(256,040)**	**0.0**	**(58,000)**		
(D) Total Continuing Budget Actions	0.0	0	0.0	0	0.0	615,544	12.4	3,551,113	12.4	3,295,073	12.4	3,237,073	**37.3**	**10,698,802**
Total Annual Project Budget Augmentation /(Reduction) [A + C]	**6.3**	**1,758,779**	**18.5**	**9,197,333**	**3.8**	**1,676,135**	**(16.2)**	**(9,081,134)**	**0.0**	**(256,040)**	**0.0**	**(58,000)**		

[A, C] Excludes Redirected Resources

97.0	**35,430,397**

Annual Savings/Revenue Adjustments

	FY 2006/07		FY 2007/08		FY 2008/09		FY 2009/10		FY 2010/11		FY 2011/12	
Cost Savings	0.0	0	0.0	0	0.0	0	67.7	3,535,803	91.8	4,796,046	72.7	3,799,065
Increased Program Revenues		0		0		0		0		0		0